NGUYỄN QUANG ANH

KHOA HỌC MÁY TÍNH

2020 – 2022

HÀ NỘI – NĂM 2022

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN QUANG ANH

NGHIÊN CỨU KỸ THUẬT TẤN CÔNG MẠNG NỘI BỘ VÀ PHƯƠNG PHÁP PHÒNG CHỐNG

LUẬN VĂN THẠC SĨ KỸ THUẬT

(*Theo định hướng ứng dụng*)

HÀ NỘI - NĂM 2022

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN QUANG ANH

NGHIÊN CỨU KỸ THUẬT TẤN CÔNG MẠNG NỘI BỘ VÀ PHƯƠNG PHÁP PHÒNG CHỐNG

Chuyên ngành: KHOA HỌC MÁY TÍNH
Mã số: 8.48.01.01

LUẬN VĂN THẠC SĨ KỸ THUẬT
(*Theo định hướng ứng dụng*)

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS.TS. ĐỖ XUÂN CHỢ

HÀ NỘI - NĂM 2022

LỜI CAM ĐOAN

Tôi tên là Nguyễn Quang Anh, xin cam đoan: Luận văn Thạc sĩ Kỹ thuật "Nghiên cứu kỹ thuật tấn công mạng nội bộ và phương pháp phòng chống" đây là công trình nghiên cứu của tác giả dưới sự hướng dẫn của PSG.TS. Đỗ Xuân Chợ. Các kết quả nghiên cứu trong luận văn là trung thực, không sao chép bất kỳ từ một nguồn nào và dưới bất kỳ hình thức nào. Các nguồn tài liệu tham khảo đã được trích dẫn và ghi nguồn đúng quy định.

Tác giả của luận văn

Nguyễn Quang Anh

LỜI CẢM ƠN

Với lòng biết ơn sâu sắc, tôi xin gửi lời cảm ơn chân thành tới những người đã giúp đỡ tôi trong quá trình học tập, nghiên cứu khoa học.

Tôi xin chân thành cảm ơn:

Trước hết tôi xin cảm ơn thầy PGS.TS. Đỗ Xuân Chợ đã nhiệt tình hướng dẫn truyền đạt những kinh nghiệm quý báu và giúp đỡ tôi từ những ngày bắt đầu hướng dẫn đến ngày bảo vệ.

Tiếp theo, tôi xin cảm ơn các thầy cô giảng viên trong Trường Học viện Công nghệ Bưu chính Viễn thông đã tận tình giảng dạy, truyền đạt những kiến thức quý báu.

Tôi xin trân trọng cảm ơn đơn vị nơi tôi công tác và làm việc đã tạo mọi điều kiện thuận lợi cho tôi trong thời gian học cao học.

Cuối cùng, tôi xin cảm ơn gia đình, đồng nghiệp, bạn bè đã luôn đồng hành, cổ vũ và giúp đỡ tôi hoàn thành luận văn này.

MỤC LỤC

MỤC LỤC ẢNH

DANH MỤC TỪ VIẾT TẮT

STT	Ký hiệu chữ viết tắt	Chữ viết đầy đủ	Dịch nghĩa
1	LAN	Local Area Network	Mạng cục bộ
2	Mbps	Megabit per second	Megabit trên giây
3	MAC	Medium Access Control	Địa chỉ vật lý
4	MITM	Man in the middle	Tấn công xe giữa
5	DDoS	Distributed Denial of Service	Tấn công từ chối dịch vụ phân tán
6	SQL	Structured Query Language	Ngôn ngữ truy vấn mang tính cấu trúc
7	ARP	Address Resolution Protocol	Giao thức truyền thông mạng với địa chỉ vật lý
8	IP	Internet Protocol	Giao thức Internet
9	WAN	Wide Area Network	Mạng diện rộng
10	CSMA	Carrier Sense Multiple Access	Đa truy cập theo cảm nhận sóng

LỜI NÓI ĐẦU

Trong những năm gần đây, sự phát triển nhanh chóng của ngành Công nghệ thông tin (CNTT) đã mang lại nhiều tiện ích trong cuộc sống. Mọi công việc trở nên nhẹ nhàng, nhanh chóng và tiện lợi hơn nhờ số hóa. Ứng dụng của CNTT được áp dụng vào hầu hết các công việc hàng ngày, từ đi chợ, mua sắm hàng hóa, học tập, làm việc, các dịch vụ công. Rất nhiều doanh nghiệp, cơ quan nhà nước đã và đang tiến hành chuyển đổi số, nhằm đem các ứng dụng CNTT vào phục vụ công việc một cách triệt để. Tuy nhiên, cùng với những lợi ích đó, sự phát triển của CNTT cũng mang đến một loại hình tội phạm mới – tội phạm sử dụng công nghệ cao. Ví dụ điển hình là những vụ tấn công vào các hệ thống máy chủ, cài cắm mã độc, virus, mã hóa các thông tin nhạy cảm để đòi tiền chuộc, hoặc nguy hiểm hơn là xâm phạm an ninh quốc phòng. Các hình thức tấn công mạng ngày càng tinh vi hơn, và không chỉ trên môi trường Internet, những hệ thống mạng nội bộ, mạng diện rộng dùng đường truyền riêng cũng có nguy cơ bị tấn công rất cao.

Đối với các công ty lớn, việc bị tấn công mạng nội bộ có thể gây thiệt hại lớn về mặt tiền bạc, còn đối với các cơ quan nhà nước, mức độ thiệt hại có thể lớn hơn rất nhiều, thậm chí có thể ảnh hưởng tới nền an ninh Quốc gia. Chính vì thế, việc nghiên cứu về các phương pháp tấn công mạng, cũng như các biện pháp để phòng thủ là vô cùng cần thiết và là nhu cầu cấp bách hiện nay. Từ những lý do như vậy, học viên lựa chọn đề tài: "**NGHIÊN CỨU KỸ THUẬT TẤN CÔNG MẠNG NỘI BỘ VÀ PHƯƠNG PHÁP PHÒNG CHỐNG**".

TỔNG QUAN VỀ ĐỀ TÀI NGHIÊN CỨU

Hiện nay các phương pháp tấn công mạng và cách ngăn chặn được phổ biến khá nhiều trên Internet, một người có chút ít kiến thức về CNTT cũng có thể tự học cách tấn công mạng trên YouTube. Tuy nhiên, hầu hết các phương pháp này đều áp dụng trên nền tảng Internet, và đối tượng chủ yếu là người dùng cuối, với các mục tiêu như cài mã quảng cáo, điều hướng người dùng đến trang web giả mạo, virus mã hóa đòi tiền chuộc, lấy thông tin cá nhân, thẻ tín dụng, tài khoản ngân hàng. Còn đối với các mạng nội bộ, không có kết nối Internet, hoặc kết nối một phần với Internet thì các phương pháp tấn công và phòng thủ lại có sự khác biệt. Khác biệt từ các phương pháp tấn công, mục tiêu tấn công và mục đích tấn công.

Đối với các tổ chức, doanh nghiệp sử dụng mạng nội bộ thường thiếu sự phòng bị và đầu tư liên quan đến việc chống tấn công mạng. Lý do chính là chủ quan về việc không kết nối Internet thì không thể tấn công được. Quan niệm trên là không chính xác, các phương pháp tấn công mạng nội bộ vẫn có thể thực hiện được dù không có kết nối tới Internet, hoặc thông qua các vùng trung gian giữa mạng nội bộ và Internet, hoặc thông qua các thiết bị ngoại vi, như USB, đĩa CD, v.v…. Mặt khác, đa phần các vụ tấn công mạng đều xảy ra rồi thì phía nạn nhân mới biết, nên thường rơi vào tình trạng bị động, lo khắc phục sự cố. Chính vì thế cần có những giải pháp để có thể chủ động chống tấn công, phát hiện trong quá trình tấn công, tránh việc luôn phải đi sau để dọn dẹp hậu quả.

Đề tài nghiên cứu các phương pháp tấn công mạng nội bộ và phương pháp phòng chống sẽ tập trung vào phân tích khái quát về mạng nội bộ, phân tích các phương pháp tấn công qua mạng LAN đồng thời chỉ ra các điểm mạnh, điểm yếu của phương pháp đó và cách để phòng thủ hiệu quả nhất. Cùng với đó là nghiên cứu một số phương pháp chống tấn công chủ động.

CHƯƠNG 1: TỔNG QUAN VỀ MẠNG NỘI BỘ

1.1. Giới thiệu về mạng nội bộ

1.1.1. Mạng nội bộ là gì

Một mạng nội bộ là một mạng riêng cho các cá nhân của một tổ chức. Thông thường, một loạt thông tin và dịch vụ có sẵn trên mạng nội bộ của một tổ chức không được công khai cho tất cả mọi người, không giống như Internet. Mạng nội bộ của công ty có thể tạo thành một đầu mối quan trọng trong giao tiếp và cộng tác nội bộ, là một điểm cung cấp thông tin làm việc tập trung để các cá nhân có thể truy cập các tài nguyên bên trong và bên ngoài. Mạng nội bộ thường được thiết lập với các công nghệ dành cho mạng cục bộ (LAN) và mạng diện rộng (WAN). Nhiều mạng nội bộ hiện đại có công cụ tìm kiếm, hồ sơ người dùng, danh bạ, blog, ứng dụng di động có thông báo và lập kế hoạch cho các sự kiện của công ty, tổ chức đó.

Hình 1.1. Mạng nội bộ

Không phải mọi cá nhân trong tổ chức đều được cấp quyền truy cập vào mạng nội bộ, chỉ những người được cấp phép mới có quyền truy cập. Một số cá nhân được phân loại truy cập dựa trên loại công việc, có thể không có nhu cầu truy cập thông tin

trên mạng nội bộ, trong đó thường liên quan đến đào tạo, cung cấp thông tin sản phẩm, chính sách, quy định và các thông tin liên quan đến tổ chức.

Hình 1.2. Xây dựng mạng nội bộ

Mạng nội bộ từ các tổ chức khác nhau thường không được kết nối với nhau. Chi khi nào các tổ chức này đồng ý chia sẻ thông tin, thì mới có kết nối đến cơ sở hạ tầng của nhau như các máy chủ, data center. Mạng nội bộ của một tổ chức được phát triển và điều hành bởi các cá nhân của chính tổ chức đó, hoặc thuê các đơn vị chuyên môn về xây dựng mạng nội bộ.

1.1.2. Cách sử dụng trong hệ thống mạng nội bộ

Ngày nay, mạng nội bộ được sử dụng để cung cấp các công cụ, tính năng, ví dụ như cộng tác để tạo điều kiện làm việc theo nhóm và hội nghị trực tiếp, hoặc các thư mục công ty, các công cụ quản lý sản phẩm, quản lý dự án, v.v…

Mạng nội bộ cũng đang được sử dụng làm nền tảng để thay đổi văn hóa trong công ty và doanh nghiệp.

Hình 1.3. Ứng dụng trong hệ thống mạng nội bộ

Trong mạng nội bộ các lưu lượng truy cập cũng thường tương tự như lưu lượng truy cập public và có thể được giám sát và phân tích bằng cách sử dụng phần mềm theo dõi giám sát. Khảo sát của người dùng cũng cải thiện hiệu quả trang web của mạng nội bộ.

Các công ty lớn cho phép người dùng truy cập vào Internet thông qua các máy chủ Proxy (Proxy Server). Chúng có khả năng sàng lọc các thông điệp đến và đi, giữ gìn an toàn mạng. Khi một phần của mạng nội bộ được cấp phép cho các khách hàng và đối tác bên ngoài công ty, nó sẽ trở thành một phần của Internet. Các mạng nội bộ khi này sẽ có các gate way để kết nối đến Internet. Các công ty sử dụng mạng nội bộ có thể gửi thông báo riêng qua mạng công cộng, sử dụng mã hóa hoặc giải mã đặc biệt và các biện pháp, chính sách bảo mật khác để kết nối một phần của mạng nội bộ của họ với các mạng khác.

Các đội phát triển, biên tập và người sử dụng phải làm việc cùng nhau để tạo ra các dịch vụ trên mạng nội bộ. Thông thường, một mạng nội bộ được quản lý bởi các bộ phận truyền thông, CIO hoặc nhân sự của các tổ chức lớn hoặc là sự kết hợp tất cả các tổ chức này.

Một mạng nội bộ đôi khi có thể phức tạp hơn nhiều so với các mạng công cộng của chính họ, do sự đa dạng và phạm vi lớn của nội dung và số lượng nút. Mạng nội bộ và việc sử dụng chúng đang phát triển nhanh chóng.

1.1.3. Lợi ích của hệ thống mạng nội bộ

- **Năng suất lao động**: Mạng nội bộ có thể giúp người dùng định vị, xem thông tin nhanh hơn và sử dụng các ứng dụng liên quan đến vai trò và công việc của họ. Giúp phần nào cải thiện năng suất lao động.
- **Linh hoạt về thời gian**: Mạng nội bộ cho phép các tổ chức phân phối thông tin cho các nhân viên trên cơ sở khi cần thiết. Còn nhân viên có thể liên kết với thông tin liên quan một cách thuận tiện, thay vì phải tìm kiếm và sắp xếp một cách lộn xộn qua email.
- **Giao tiếp dễ dàng**: Mạng nội bộ có thể đóng vai trò là công cụ quan trọng để liên lạc, giao tiếp trong một tổ chức, các sáng kiến chiến lược có phạm vi toàn cầu trong tất cả các tổ chức. Thông tin có thể dễ dàng truyền đạt, sáng kiến và mục đích của sáng kiến cần đạt được và ai đang thúc đẩy sáng kiến, kết quả đạt được. Một số ví dụ về giao tiếp là trò chuyện qua email hoặc các công cụ chat, hội nghị truyền hình.
- **Xây dựng website**: Cho phép thông tin kiến thức doanh nghiệp có tính chất phức tạp được duy trì và dễ dàng truy cập trong toàn công ty bằng cách sử dụng các ứng dụng website. Ví dụ bao gồm: hướng dẫn nhân viên, quyền lợi, chính sách công ty, nguồn cấp thông tin hoặc tài liệu đào tạo, có thể được truy cập bằng các tiêu chuẩn Internet phổ biến. Thông qua website, các công ty có thể dễ dàng cập nhật và điều chỉnh các chính sách, nội dung các tài liệu, và nhân viên có thể trực tiếp xem và tải các phiên bản mới nhất.

- **Hoạt động kinh doanh và quản lý kinh doanh**: Mạng nội bộ cũng đang được sử dụng như một nền tảng để phát triển và triển khai các ứng dụng hỗ trợ các hoạt động quản lý, báo cáo, thông kê của doanh nghiệp.
- **Quy trình làm việc**: giảm độ chậm trễ, chẳng hạn như tự động lên lịch họp hoặc lên kế hoạch nghỉ phép, nhắc nhở công việc, chấm điểm KPI
- **Tiết kiệm về chi phí**: Người dùng có thể xem thông tin và dữ liệu qua trình duyệt web thay vì duy trì các tài liệu trên giấy như trước, danh bạ điện thoại nội bộ và biểu mẫu trưng dụng bằng giấy in. Điều này giúp tiết kiệm chi phí kinh doanh cho việc in ấn, sao chép tài liệu và góp phần giúp bảo vệ môi trường cũng như chi phí bảo trì các tài liệu.
- **Tăng cường về hợp tác**: Các thông tin có thể dễ dàng truy cập bởi tất cả người dùng được ủy quyền và cho phép làm việc theo nhóm. Cũng có thể giao tiếp trong thời gian thực tế thông qua các công cụ tích hợp của bên thứ ba, chẳng hạn như thông điệp tin nhắn tức thời, thúc đẩy chia sẻ ý tưởng và loại bỏ các khó khăn trong giao tiếp để giúp tăng năng suất của công ty.
- **Đa nền tảng**: Cụ thể là các trình duyệt web tuân thủ tiêu chuẩn có sẵn cho các hệ điều hành Windows, UNIX, Mac và Linux.
- **Được xây dựng cho đối tượng**: Các công ty đưa ra thông số kỹ thuật, do đó có thể cho phép các nhà phát triển mạng nội bộ xây dựng các ứng dụng chỉ phải hoạt động trên trình duyệt. Do Intranet là dành riêng cho một số người dùng (yêu cầu xác thực cơ sở dữ liệu hoặc mạng trước khi truy cập), biết chính xác người đang can thiệp, có thể cá nhân hóa mạng nội bộ dựa trên vai trò (chức danh, bộ phận) hoặc chỉ cá nhân.
- **Quảng bá văn hóa công ty**: Tất cả người dùng đều có khả năng xem cùng một thông tin trong hệ thống mạng nội bộ.
- **Cập nhật ngay lập tức**: Khi giao tiếp với người dùng ở bất kỳ phương diện nào ví dụ như thông số kỹ thuật, mạng nội bộ giúp cho nhân viên có thể cập nhật ngay những thay đổi mới nhất.

1.2. Công nghệ truyền dẫn mạng dây Ethernet

1.2.1. Khái niệm về Ethernet

Ethernet là một công nghệ mạng truyền gồm các công nghệ mạng dựa trên khung dữ liệu (frame-based) dành cho mạng LAN. Cái tên Ethernet xuất phát từ khái niệm của vật lý (Ether).

Ethernet là định nghĩa cho các chuẩn nối dây và phát tín hiệu ở tầng vật lý, hai phương tiện để truy nhập mạng tại phần MAC (để điều khiển truy nhập môi trường truyền dẫn) trên tầng liên kết dữ liệu, và một định dạng chung cho việc đánh các địa chỉ.

Ethernet là một công nghệ mạng cục bộ (LAN) nhằm chuyển các thông tin dữ liệu giữa các máy tính với tốc độ từ 10 đến 100 triệu bit một giây (Mbps).

Hiện nay, công nghệ Ethernet được sử dụng nhiều nhất là công nghệ sử dụng là cáp đôi xoắn 100Mbps. Với công nghệ truyền thông là 100Mbps sử dụng cáp đồng trục, cáp quang, mạng không dây. Do đó tốc độ chuẩn cho hệ thống Ethernet hiện nay sẽ là 100Mbps.

1.2.2. Ethernet là một công nghệ mạng thiết bị và rộng rãi

Ngày nay mặc dù có nhiều công nghệ LAN ra đời nhưng Ethernet vẫn là công nghệ được sử dụng rộng rãi nhất. Vào năm 2018, các nhà phân tích đã thống kê có khoảng hơn 350 triệu nút mạng Giga Ethernet đã và đang được sử dụng trên toàn thế giới, còn Ethernet 100Mpbs đã phổ cập đến hơn 80% dân số thế giới (Theo Viavi Solutions).

Kể từ khi Ethernet ra đời, các đặc tính về kĩ thuật và trình tự để xây dựng nên một mạng nội bộ đã trở nên dễ tiếp cận hơn đối với tất cả mọi người. Cùng với đặc tính dễ sử dụng đã tạo nên những hệ thống mạng nội bộ rộng lớn và là sự bắt đầu cho việc ứng dụng rộng rãi của Ethernet trong các nền công nghiệp hiện đại.

Ngày nay, các nhà sản xuất cho máy tính thường trang bị cho sản phẩm của họ thiết bị 100Mbps Ethernet khiến cho thiết bị của họ có thể sẵn sàng kết nối vào mạng Ethernet. Và khi chuẩn Ethernet 100Mbps đã trở nên rất phổ biến thì máy tính được trang bị các thiết bị Ethernet hoạt động ở cả hai tốc độ 10Mbps, 100Mbps. Những quản trị viên mạng Ethernet ngày nay cần thiết phải biết kết hợp một số lượng lớn các máy tính lại với nhau bằng công nghệ mạng qua thiết bị trung gian. Vì sử dụng chuẩn chung như vậy, nên các thiết bị dù sản xuất bởi các hãng khác nhau cũng đều có thể kết nối một cách dễ dàng.

1.2.3. Lịch sử phát triển của Ethernet

Ethernet đã được phát minh ra tại trung tâm nghiên cứu Xerox Palo Alto vào những năm 1971 bởi tiến sĩ Robert M. Metcalfe. Ban đầu, Ethernet được thiết kế với mục đích chính là phục vụ nghiên cứu trong hệ thống quản lý công ty. Trạm Ethernet đầu tiên chạy với tốc độ xấp xỉ là 3Mbps. Năm 1980, Ethernet được chính thức công bố bởi liên minh DEC-Intel-Xerox (DIX). Nỗ lực này đã chuyển "tiền thân Ethernet" trở thành một hệ thống mở Ethernet và có chất lượng với tốc độ lên tới 10Mbps. Công nghệ Ethernet sau đó đã được ban tiêu chuẩn LAN của Viện kỹ thuật điện và điện tử thế giới (IEEE 802) công nhận. Chuẩn IEEE đã được thành lập lần đầu tiên vào năm 1985, với tiêu đề "IEEE 802.3 khuyến nghị về lớp vật lý và phương thức truy nhập đa truy nhập sóng mang phát hiện va chạm". Chuẩn IEEE đã được thừa nhận bởi tổ chức tiêu chuẩn hóa của thế giới (ISO).

Chuẩn IEEE cung cấp Ethernet kiểu hệ thống dựa trên nền là công nghệ DIX Ethernet. Tất cả các hệ thống Ethernet từ năm 1985 trở đi đều được xây dựng dựa trên tiêu chuẩn IEEE 802.3. Nói chính xác hơn, chúng ta đã dựa trên công nghệ "IEEE 802.3 CSMA/CD".

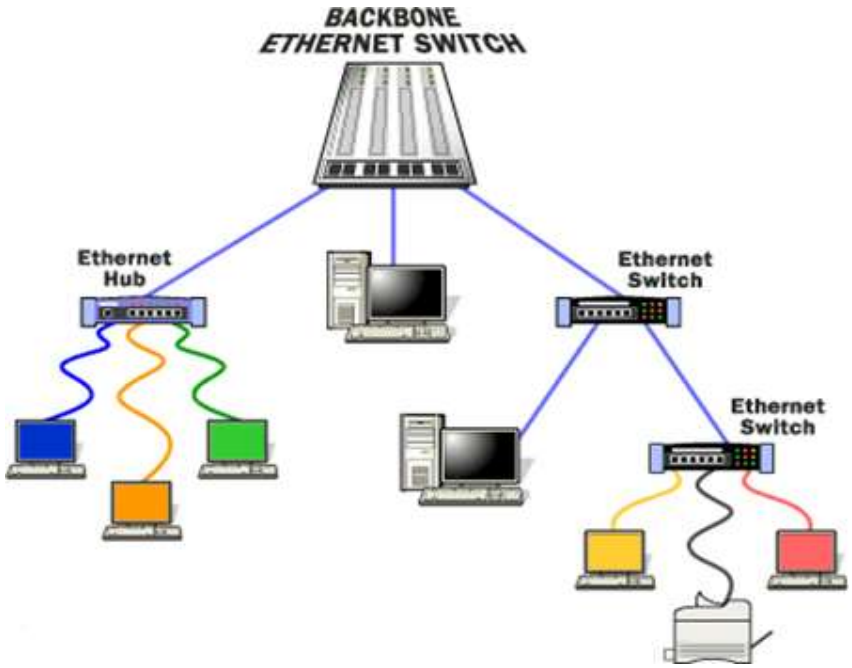
Chuẩn 802.3 được nâng cấp từng bước bao gồm các tiêu chuẩn công nghệ mới. Từ đó, năm 1985 Ethernet đã được tăng cường sức mạnh của công nghệ 10Mbps (ví dụ cáp xoắn) cũng như các khuyến nghị mới về mạng Fast Ethernet 100Mbps.

1.2.4. Các thành phần của Ethernet

Hệ thống Ethernet bao gồm 3 thành phần cơ bản:

- Ở hệ thống ở trung gian truyền tín hiệu Ethernet giữa các máy tính với nhau.
- Nhóm thiết bị trung gian sẽ đóng vai trò là giao diện Ethernet làm cho nhiều máy tính có thể kết nối tới cùng 1 kênh.
- Còn các khung Ethernet sẽ đóng vai trò là các bit chuẩn để luân chuyển dữ liệu trên Ethernet.

Sau đây sẽ miêu tả quy tắc thiết lập cho các thành phần đầu tiên, các mảng truyền thông vật lí và thiết lập quy tắc truy cập trung gian cho Ethernet và các khung Ethernet.



Hình 1.4. Các thành phần của Ethernet

1.2.5. Hoạt động của Ethernet

Các máy Ethernet (còn được gọi là máy trạm) hoạt động độc lập với tất cả các trạm khác trên mạng và không có một trạm điều khiển trung tâm. Tất cả trạm đều kết nối với Ethernet thông qua một đường truyền chung hay còn gọi là trung gian. Sau

đó để gửi dữ liệu trước tiên trạm cần lắng nghe xem kênh có rảnh rỗi không, nếu rảnh thì mới gửi đi các gói (dữ liệu).

Để tham gia được vào truyền là bằng nhau đối với mỗi trạm. Tức là không có sự ưu tiên thì sự thâm nhập vào kênh chung được quyết định bởi nhóm điều khiển truy nhập trung gian (còn được gọi là Medium Access Control-MAC) sẽ được đặt trong mỗi trạm, từ đó MAC thực thi dựa trên cơ sở sự phát hiện va chạm sóng mang (CSMA/CD).

-Giao thức CSMA/CD.

- Xung đột

-Truyền dữ liệu

1.2.6. Sự khác nhau giữa Internet và Ethernet

Ethernet:

Công nghệ mạng được coi là tiêu chuẩn nhất hiện nay và được sử dụng trong hầu hết các công ty kinh doanh. Các máy tính được kết nối với nhau thông qua 1 loại cáp đặc biệt và 1 thiết bị gọi là mecca Do sử dụng tốc độ cao trong kỹ thuật truyền cơ bản (kênh đơn). Ethernet cho phép truyền dữ liệu dạng chuỗi với tốc độ 10megabit mỗi giây, với thông số thực tế từ 2 đến 3megabit mỗi giây. Ethernet sử dụng kỹ thuật thâm nhập nhiều mối bằng cảm nhận sóng mang dò xung đột (CSMA/ CD) để đề phòng khung lưới cho mạng khi có hai thiết bị đồng thời cố gắng thâm nhập mạng.

Internet

Hệ thống bao gồm các máy tính trong một mạng được kết nối với nhau trên toàn thế giới, cho phép các dịch vụ truyền dữ liệu như đăng nhập từ xa, truyền và gửi tập tin email. Internet là một cách kết nối các mạng máy tính để chúng ta có thể nhìn thấy bức tranh toàn cảnh về cách thức hoạt động của từng hệ thống.

Hầu như ai cũng có thể tham gia Internet. Ngày nay dịch vụ Internet đã trở nên phổ biến và trở thành nhu cầu hàng ngày của mọi người. Thông qua các nhà cung cấp

dịch vụ ISP (Internet Service Provider) hoặc các công ty viễn thông sử dụng mạng không giây 3G, 4G, 5G. Ngày nay người dùng Internet còn có thể kết nối tại những nơi hoang vu thông qua chảo vệ tinh Starlink của công ty Tesla.

1.3. Kỹ thuật chuyển mạch trong mạng nội bộ

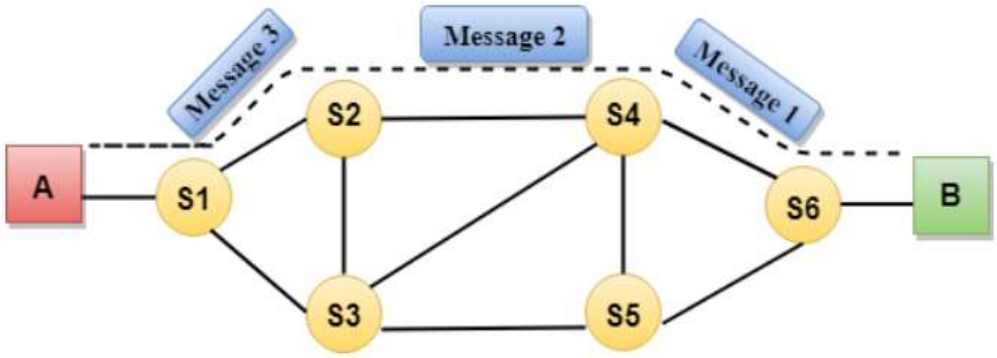
1.3.1. Khái niệm chuyển mạch

Chuyển mạch:

- Chuyển mạch kênh là một kỹ thuật thiết lập một đường dẫn riêng giữa người gửi và người nhận.
- Trong Kỹ thuật chuyển mạch, một khi kết nối được thiết lập thì đường dẫn dành riêng sẽ vẫn tồn tại cho đến khi kết nối bị ngắt.
- Chuyển mạch kênh trong mạng hoạt động theo cách tương tự như hoạt động của điện thoại.
- Một đường dẫn end-to-end hoàn chỉnh phải tồn tại trước khi quá trình giao tiếp diễn ra.
- Đối với kỹ thuật chuyển mạch kênh, khi người dùng muốn gửi dữ liệu, thoại, video, tín hiệu yêu cầu được gửi đến máy thu thì máy thu sẽ gửi lại báo nhận để đảm bảo tính khả dụng của đường dẫn chuyên dụng. Sau khi nhận được xác nhận, đường dẫn dành riêng sẽ chuyển dữ liệu.
- Chuyển mạch kênh được sử dụng trong mạng công cộng. Nó được sử dụng để truyền giọng nói.
- Dữ liệu cố định có thể được chuyển tại một thời điểm trong công nghệ chuyển mạch kênh.

Giao tiếp thông qua chuyển mạch kênh có 3 pha:

- Thành lập mạch
- Truyền dữ liệu
- Ngắt kết nối mạch



Hình 1.5. Giao tiếp thông qua chuyển mạch

1.3.2. Các công nghệ chuyển mạch

Chuyển mạch phân chia không gian:

- Chuyển mạch phân chia không gian là một công nghệ chuyển mạch kênh trong đó một đường truyền duy nhất được thực hiện trong một bộ chuyển mạch bằng cách sử dụng một tập hợp các điểm chéo riêng biệt về mặt vật lý.
- Có thể đạt được Chuyển đổi Phân chia Không gian bằng cách sử dụng chuyển mạch thanh ngang. Chuyển mạch thanh ngang là một điểm giao nhau bằng kim loại hoặc cổng bán dẫn có thể được bật hoặc tắt bởi một bộ phận điều khiển.
- Chuyển mạch Crossbar được thực hiện bằng cách sử dụng chất bán dẫn. Ví dụ, chuyển mạch xà ngang Xilinx sử dụng FPGA.
- Chuyển mạch phân chia không gian có tốc độ cao, dung lượng lớn và chuyển mạch không chặn.

Chuyển mạch phân chia không gian có thể được phân loại theo hai cách:

- Chuyển mạch xà ngang
- Chuyển mạch đa tầng

Chuyển mạch Crossbar

Chuyển mạch Crossbar là chuyển mạch có n đường vào và n đường ra. Chuyển mạch xà ngang có n2 điểm giao nhau được gọi là điểm giao nhau.

Nhược điểm của chuyển mạch Crossbar:

Số lượng các điểm giao nhau tăng lên khi số lượng các trạm được tăng lên. Do đó, nó trở nên rất đắt đối với một chuyển mạch lớn. Giải pháp cho điều này là sử dụng một chuyển mạch nhiều tầng.

Chuyển mạch đa tầng

Chuyển mạch đa tầng được thực hiện bằng cách chia chuyển mạch xà ngang thành các đơn vị nhỏ hơn và sau đó kết nối chúng với nhau. Nó làm giảm số lượng các điểm giao nhau. Nếu một đường dẫn không thành công, thì sẽ có sẵn đường dẫn khác.

Ưu điểm của chuyển mạch:

- Trong trường hợp của kỹ thuật Chuyển mạch, kênh liên lạc được dành riêng.
- Nó có băng thông cố định.

Nhược điểm của chuyển mạch:

- Khi đường dẫn dành riêng được thiết lập, độ trễ duy nhất xảy ra đối với tốc độ truyền dữ liệu.
- Mất một thời gian dài để thiết lập kết nối, khoảng 10 giây trong đó không có dữ liệu nào có thể được truyền.
- Nó đắt hơn các kỹ thuật chuyển mạch khác vì cần có một đường dẫn dành riêng cho mỗi kết nối.
- Nó không hiệu quả để sử dụng vì một khi đường dẫn được thiết lập và không có dữ liệu nào được truyền đi, thì dung lượng của đường dẫn sẽ bị lãng phí.
- Trong trường hợp này, kết nối là dành riêng, do đó không thể truyền dữ liệu nào khác ngay cả khi kênh miễn phí.

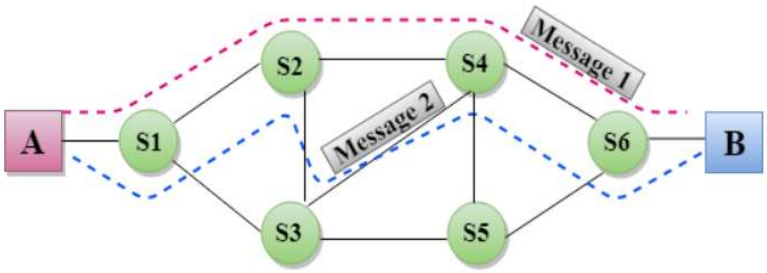
Chuyển mạch thông điệp

Chuyển mạch thông điệp là một kỹ thuật chuyển mạch trong đó thông điệp được chuyển như một đơn vị hoàn chỉnh và được định tuyến qua các nút trung gian mà tại đó nó được lưu trữ và chuyển tiếp.

Trong kỹ thuật chuyển mạch thông điệp, không có thiết lập đường dẫn riêng giữa người gửi và người nhận.

Địa chỉ đích được thêm vào tin nhắn. Chuyển mạch thông điệp cung cấp một định tuyến động vì thông báo được định tuyến qua các nút trung gian dựa trên thông tin có sẵn trong thông báo.

Chuyển mạch thông điệp được lập trình theo cách để chúng có thể cung cấp các tuyến đường hiệu quả nhất. Mỗi và mọi nút đều lưu trữ toàn bộ thông điệp và sau đó chuyển tiếp nó đến nút tiếp theo. Loại mạng này được gọi là mạng cửa hàng và mạng chuyển tiếp. Chuyển mạch thông điệp coi mỗi tin nhắn như một thực thể độc lập.



Hình 1.6. Chuyển mạch thông điệp

Ưu điểm Chuyển mạch thông điệp:

- Kênh dữ liệu được chia sẻ giữa các thiết bị giao tiếp giúp cho cải thiện hiệu quả sử dụng băng thông.
- Tắc nghẽn giao thông có thể được giảm bớt vì thông báo được lưu trữ tạm thời trong các nút.

- Ưu tiên tin nhắn có thể được sử dụng để quản lý mạng.
- Kích thước của tin nhắn được gửi qua mạng có thể khác nhau. Do đó, nó hỗ trợ dữ liệu có kích thước không giới hạn.

Nhược điểm của Chuyển mạch thông điệp

- Các chuyển mạch tin nhắn phải được trang bị đủ dung lượng để cho phép chúng lưu tin nhắn cho đến khi tin nhắn được chuyển tiếp.
- Độ trễ lâu có thể xảy ra do phương tiện lưu trữ và chuyển tiếp được cung cấp bởi kỹ thuật chuyển mạch bản tin.

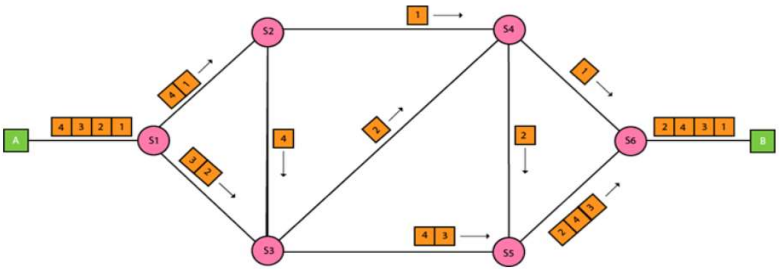
Chuyển mạch gói

Chuyển mạch gói là một kỹ thuật chuyển mạch trong đó thông điệp được gửi trong một lần, nhưng nó được chia thành nhiều phần nhỏ hơn và chúng được gửi riêng lẻ.

Thông điệp được chia thành các phần nhỏ hơn được gọi là các gói và các gói được cung cấp một số duy nhất để xác định thứ tự của chúng ở đầu nhận.

Mỗi gói chứa một số thông tin trong tiêu đề của nó như địa chỉ nguồn, địa chỉ đích và số thứ tự. Các gói sẽ di chuyển trên mạng, đi theo đường ngắn nhất có thể. Tất cả các gói được tập hợp lại ở đầu nhận theo đúng thứ tự.

Nếu bất kỳ gói nào bị thiếu hoặc bị hỏng, thì thông báo sẽ được gửi đi để gửi lại tin nhắn. Nếu đạt được thứ tự chính xác của các gói, thì thông báo xác nhận sẽ được gửi.



Hình 1.7. Chuyển mạch gói

Các phương pháp chuyển đổi gói

Có hai cách tiếp cận để chuyển đổi gói:

Chuyển mạch gói dữ liệu:

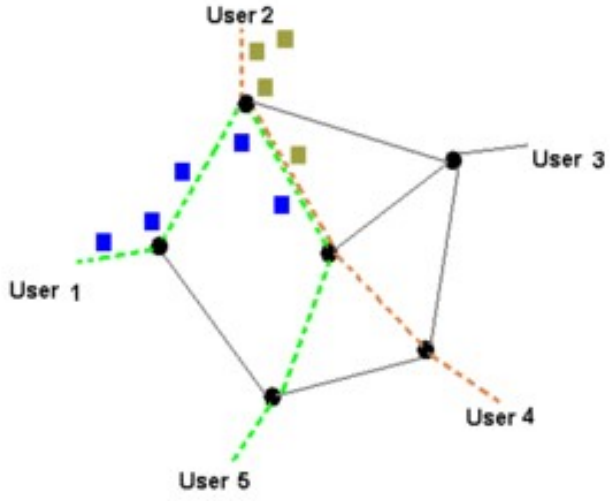
Nó là một công nghệ chuyển mạch gói trong đó gói được biết đến như một gói dữ liệu, được coi như một thực thể độc lập. Mỗi gói chứa thông tin về đích và bộ chuyển mạch sử dụng thông tin này để chuyển gói đến đúng đích.

Các gói được tập hợp lại ở đầu nhận theo đúng thứ tự. Trong kỹ thuật chuyển mạch gói dữ liệu, đường dẫn không cố định. Các nút trung gian thực hiện các quyết định định tuyến để chuyển tiếp các gói tin. Datagram Packet Switching còn được gọi là chuyển mạch không kết nối.

Chuyển mạch ảo

Chuyển mạch ảo còn được gọi là chuyển mạch hướng kết nối. Trong trường hợp Chuyển mạch kênh ảo, một lộ trình dự kiến trước được thiết lập trước khi các thông điệp được gửi đi. Các gói yêu cầu cuộc gọi và chấp nhận cuộc gọi được sử dụng để thiết lập kết nối giữa người gửi và người nhận. Trong trường hợp này, đường dẫn được cố định trong khoảng thời gian của một kết nối logic.

Hãy hiểu khái niệm chuyển mạch ảo qua sơ đồ:



Hình 1.8. Chuyển mạch ảo

Trong sơ đồ trên, A và B lần lượt là người gửi và người nhận. 1 và 2 là các nút. Các gói yêu cầu cuộc gọi và chấp nhận cuộc gọi được sử dụng để thiết lập kết nối giữa người gửi và người nhận. Khi một tuyến đường được thiết lập, dữ liệu sẽ được chuyển. Sau khi truyền dữ liệu, người nhận sẽ gửi tín hiệu báo nhận rằng tin nhắn đã được nhận. Nếu người dùng muốn chấm dứt kết nối, một tín hiệu rõ ràng sẽ được gửi cho việc chấm dứt.

Ưu điểm của chuyển mạch gói:

- Hiệu quả về chi phí: Trong kỹ thuật chuyển mạch gói, các thiết bị chuyển mạch không yêu cầu bộ nhớ thứ cấp lớn để lưu trữ các gói, do đó chi phí được giảm thiểu ở một mức độ nào đó. Do đó, có thể nói rằng kỹ thuật chuyển mạch gói là một kỹ thuật tiết kiệm chi phí.

- Đáng tin cậy: Nếu bất kỳ nút nào đang bận, thì các gói tin có thể được định tuyến lại. Điều này đảm bảo rằng kỹ thuật chuyển mạch gói cung cấp thông tin liên lạc đáng tin cậy.

- Hiệu quả: Chuyển mạch gói là một kỹ thuật hiệu quả. Nó không yêu cầu bất kỳ đường dẫn thiết lập nào trước khi truyền và nhiều người dùng có thể sử dụng cùng một kênh liên lạc đồng thời, do đó sử dụng rất hiệu quả băng thông có sẵn.

Nhược điểm của chuyển mạch gói:

- Kỹ thuật chuyển mạch gói không thể được thực hiện trong những ứng dụng yêu cầu độ trễ thấp và dịch vụ chất lượng cao.
- Các giao thức được sử dụng trong kỹ thuật chuyển mạch gói rất phức tạp và đòi hỏi chi phí thực hiện cao.
- Nếu mạng bị quá tải hoặc bị hỏng, thì nó yêu cầu truyền lại các gói bị mất. Nó cũng có thể dẫn đến việc mất thông tin quan trọng nếu các lỗi không được khôi phục.

1.4. Kết luận Chương 1

Kết thúc Chương 1, luận văn đã nghiên cứu tổng quan về mạng nội bộ và các kỹ thuật sử dụng trong mạng nội bộ, bao gồm: khái niệm mạng nội bộ, lợi ích của mạng nội bộ, khá niệm về công nghệ Ethernet và các kỹ thuật liên quan. Ngoài ra, luận văn cũng đã nghiên cứu và tìm hiểu về chuyển mạch và một số công nghệ chuyển mạch.

Từ những nghiên cứu về mạng nội bộ và các kỹ thuật chuyển mạch, học viên nhận thấy mạng nội bộ có cấu trúc rất phức tạp và có nhiều thiết bị cấu thành một mạng nội bộ. Đồng thời các kỹ thuật chuyển mạch cũng rất đa dạng và tồn tại nhiều nhược điểm. Điều này dẫn đến việc nguy cơ bị tấn công mạng thông qua các thiết bị thành phần và trong chính các kỹ thuật chuyển mạch, định tuyến. Chính vì vậy vì vậy, cần phải nghiên cứu các phương thức tấn công mạng nội bộ để đưa ra giải pháp phòng chống.

CHƯƠNG 2: TẤN CÔNG MẠNG NỘI BỘ VÀ GIẢI PHÁP PHÒNG CHỐNG

2.1. Tổng quan về an toàn bảo mật thông tin

An ninh mạng ngày càng trở nên quan trọng hơn khi điện thoại thông minh, máy tính và máy tính bảng trở thành một phần không thể thiếu trong công việc hàng ngày và cuộc sống cá nhân. Mức độ phụ thuộc vào các công cụ trực tuyến trong các khía cạnh khác nhau của hoạt động kinh doanh – từ mạng xã hội và tiếp thị qua email đến lưu trữ dữ liệu nhân viên và khách hàng trên đám mây – đặt ra nhu cầu bổ sung trong việc bảo vệ những thông tin quý giá này**.**

Sự phụ thuộc vào các công cụ số khiến nhiều doanh nghiệp gặp rủi ro từ các cuộc tấn công mạng. Kiến thức vững chắc về an ninh mạng là chìa khóa ở đây, vì các cuộc tấn công như vậy vẫn không ngừng phát triển và ngày càng tinh vi hơn. Nạn nhân của các cuộc tấn công mạng có thể có nguy cơ:

- Mất dữ liệu nhạy cảm
- Tổn thất tài chính do trộm cắp dữ liệu
- Chi phí cao cho việc khôi phục dữ liệu bị đánh cắp
- Mất đi danh tiếng
- Đóng cửa (trong trường hợp nghiêm trọng)

Với sự phát triển của việc sử dụng Internet, các công cụ trực tuyến và các thiết bị liên quan, tội phạm mạng đã lan rộng trong các tổ chức, doanh nghiệp. Vì an ninh mạng không có giải pháp chung cho tất cả, chúng ta cần xem xét các lĩnh vực khác nhau có liên quan đến doanh nghiệp của mình, dữ liệu và nơi nó được lưu trữ trực tuyến.

Có nhiều loại tấn công mạng công khai và âm thầm – cả hai đều được thiết kế để làm gián đoạn hoạt động của doanh nghiệp, tổ chức theo nhiều cách thức khác nhau. Khi ngày càng có nhiều công ty nhận thức được tầm quan trọng của việc bảo vệ tài nguyên của họ và thực hiện đào tạo về an ninh mạng, thì tin tặc và tội phạm mạng cũng đang phát triển các hình thức tấn công khác ngày càng tinh vi hơn.

Bằng cách cập nhật kiến thức của mình, chúng ta có thể bảo vệ doanh nghiệp của mình khỏi chúng tốt hơn. Có năm loại tấn công mạng phổ biến nhất:

- **Malware**: Là một lỗ hổng trên hệ thống bảo vệ mạng, chẳng hạn như phần mềm gián điệp, phần mềm tống tiền và vi rút.
- **Phishing**: Là những tin nhắn độc hại (thường là email) chứa các liên kết độc hại mà khi được nhấp vào, chúng sẽ gửi quyền truy cập vào thông tin nhạy cảm.
- **Denial of Service (DoS)**: Tin tặc tràn ngập mạng hoặc hệ thống với nhiều thông tin dư thừa nhằm làm quá tải và buộc hệ thống phải dừng hoạt động.
- **Man in the middle (MitM)**: Tội phạm mạng làm gián đoạn kết nối, thường là qua mạng wi-fi công cộng không an toàn và sau đó đánh cắp dữ liệu nhạy cảm.
- **Zero-day attack:** Một cuộc tấn công ít phổ biến hơn nhưng xảy ra ngày càng nhiều giữa việc công bố bản cập nhật hoặc bản vá bảo mật và cài đặt của nó.

Những kiểu tấn công mạng này có thể ảnh hưởng đến nhiều doanh nghiệp, chẳng hạn như quán cà phê có mạng wi-fi không an toàn hoặc các shop online có nguy cơ bị tấn công zero-day.

2.2. Một số kỹ thuật tấn công mạng nội bộ

2.2.1. Tấn công sử dụng phần mềm độc hại (Malware)

Các cuộc tấn công bằng phần mềm độc hại là hình thức phổ biến và phổ biến nhất. Chúng bao gồm phần mềm gián điệp (gián điệp), ransomware (mã độc) và sâu (phần mềm độc hại có thể lây lan sang các thiết bị khác). Những kẻ tấn công thường sử dụng các lỗ hổng bảo mật để nhắm mục tiêu người dùng. Nó có thể lừa nạn nhân nhấp vào liên kết và tự động cài đặt phần mềm độc hại trên máy tính của họ. Một khi được cài đặt thành công, malware sẽ gây ra.

- Ngăn cản người dùng truy cập vào một đường link quan trọng (ransomware)
- Cài đặt thêm những phần mềm độc hại khác

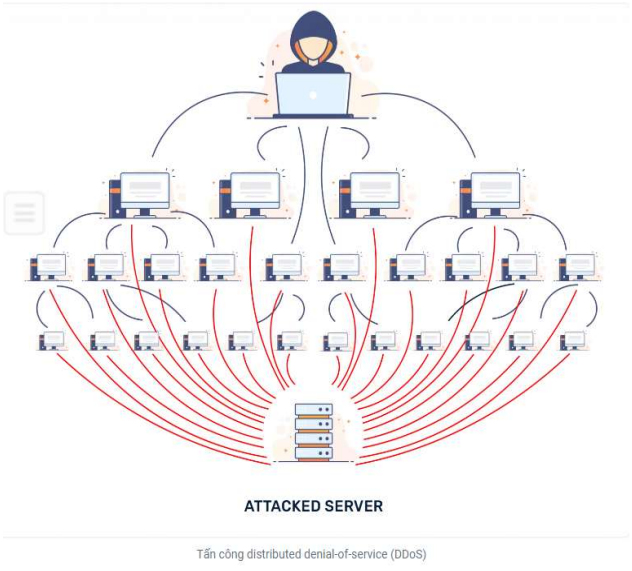
- Nghe lén người dùng và đánh cắp dữ liệu (spyware)
- Phá hỏng phần mềm, phần cứng, làm gián đoạn hệ thống.

2.2.2. Tấn công giả mạo (Phishing)

Phishing là một kiểu tấn công chiếm được lòng tin của người dùng bằng cách mạo danh một cá nhân hoặc tổ chức hợp pháp, thường thông qua tin nhắn văn bản hoặc email. Các cuộc tấn công Phishing thường cố gắng đánh cắp dữ liệu và thông tin nhạy cảm của nạn nhân, chẳng hạn như số thẻ tín dụng và mật khẩu. Phishing có thể là một hình thức lừa người dùng cài đặt phần mềm độc hại trên thiết bị của họ từ đó. Phishing là một phần trong tấn công malware.

2.2.3. Tấn công từ chối dịch vụ (DoS và DDoS)

Một cuộc tấn công DDos sẽ chiếm đoạt tài nguyên (resource) của hệ thống khiến nó không thể phản hồi các yêu cầu dịch vụ. Cuộc tấn công DDoS cũng là một cuộc tấn công vào tài nguyên của hệ thống, nhưng nó được thực hiện từ một số lượng lớn các host khác mà bị nhiễm phần mềm độc hại do hacker kiểm soát.



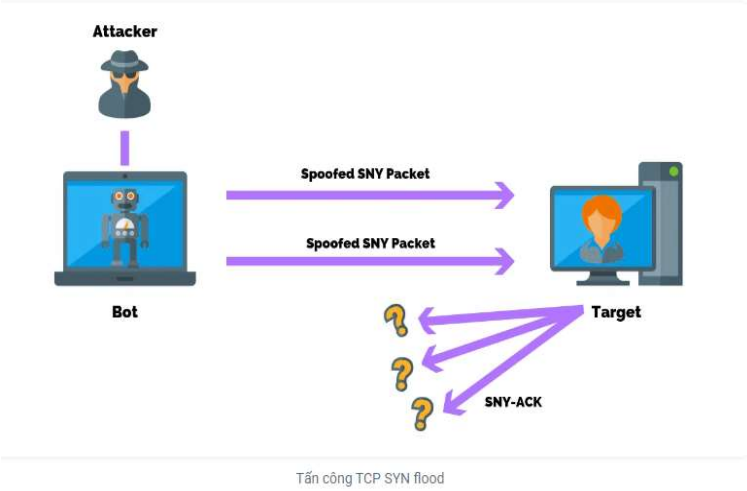
Hình 2.1. Tấn công DDoS

Không giống như các cuộc tấn công được tạo ra để cho phép kẻ tấn công có được quyền truy cập, DDoS không mang lại lợi ích trực tiếp cho kẻ tấn công. Đối với một số hacker, chỉ cần đạt được việc từ chối dịch vụ là đủ hài lòng. Tuy nhiên, nếu resource bị tấn công thuộc về một đối thủ cạnh tranh kinh doanh, thì lợi ích mang lại cho kẻ tấn công là không hề nhỏ. Một mục đích khác của tấn công DDoS có thể là đưa một hệ thống offline để có thể khởi chạy một loại tấn công khác. Điển hình là chiếm quyền điều khiển hijacking.

Có nhiều kiểu tấn công DoS và DDoS khác nhau, phổ biến nhất là tấn công TCP SYN flood, tấn công Teardrop, tấn công Smurf, tấn công ping-of-death và botnet.

Tấn công TCP SYN flood

Trong cuộc tấn công này, hacker khai thác việc sử dụng bộ nhớ buffer trong quá trình handshake khởi tạo phiên bản TCP (Transmission Control Protocol). Hacker làm quá tải queue in-process của hệ thống mục tiêu với các yêu cầu kết nối, nhưng nó không phản hồi khi hệ thống mục tiêu trả lời các yêu cầu đó. Điều này khiến hệ thống mục tiêu hết thời gian chờ đợi phản hồi từ thiết bị của kẻ tấn công, điều này khiến hệ thống gặp sự cố hoặc không sử dụng được vì hàng đợi queue bị đầy.



Hình 2.2. Tấn công TCP SYN flood

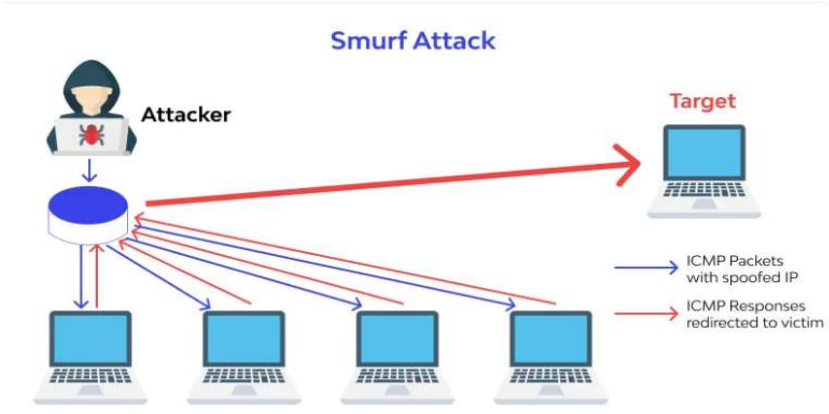
Tấn công Teardrop

Cuộc tấn công này làm cho các trường độ dài và độ lệch phân mảnh trong các gói Internet Protocol (IP) tuần tự chồng lên nhau trên host bị tấn công. Mặc dù hệ thống bị tấn công cố gắng tạo lại các gói trong quá trình này nhưng không thành công. Hệ thống mục tiêu sau đó trở nên nhầm lẫn và bị treo.

Hình 2.3. Tấn công Teardrop

Nếu người dùng không có các bản vá (patch) để bảo vệ khỏi cuộc tấn công DDoS này, hãy vô hiệu hóa SMBv2 và chặn các cổng port 139 và 445.

Tấn công Smurf

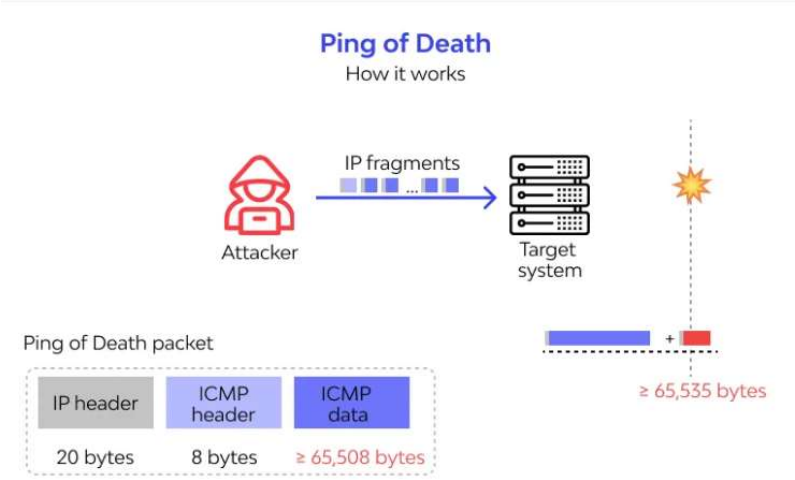


Hình 2.4. Tấn công Smurf

Để bảo vệ thiết bị khỏi cuộc tấn công như thế này, chúng ta cần phải tắt các broadcast IP được phát trực tiếp tại các bộ định tuyến router. Điều này sẽ ngăn chặn yêu cầu broadcast ICMP echo trên các thiết bị mạng. Một tùy chọn khác là định cấu hình hệ thống cuối để ngăn chúng phản hồi các gói ICMP từ các địa chỉ broadcast.

Tấn công Ping of Death

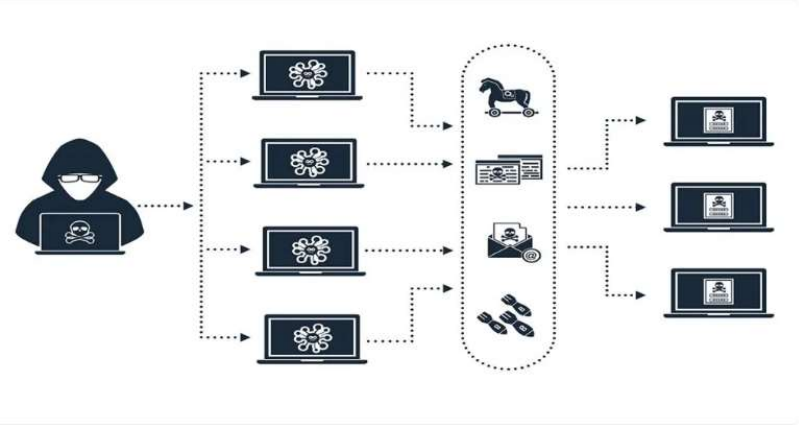
Loại tấn công này sử dụng các gói IP để ping một hệ thống mục tiêu có kích thước IP tối đa là 65,535 byte. Các gói IP có kích thước này không được cho phép, vì vậy hacker sẽ phân mảnh gói IP. Khi hệ thống mục tiêu tập hợp lại gói tin, nó có thể bị quá tải bộ đệm và các sự cố khác.



Hình 2.5. Tấn công Ping Of Dead

Botnet

Botnet là hàng triệu hệ thống bị nhiễm phần mềm độc hại dưới sự kiểm soát của hacker để thực hiện các cuộc tấn công DDoS. Các bot hoặc hệ thống zombie này được sử dụng để thực hiện các cuộc tấn công chống lại hệ thống mục tiêu, thường làm quá tải băng thông bandwidth và khả năng xử lý của hệ thống mục tiêu. Các cuộc tấn công DDoS này rất khó truy dấu vết vì các botnet nằm ở nhiều vị trí địa lý khác nhau.



Hình 2.6. Tấn công Botnet

Botnet có thể được giảm thiểu bằng cách:

Lọc RFC3704, nơi mà sẽ từ chối lưu lượng truy cập từ các địa chỉ giả mạo (spoof) và giúp đảm bảo rằng lưu lượng truy cập có thể truy dấu đến đúng mạng nguồn của nó. Ví dụ, bộ lọc RFC3704 sẽ để các gói từ địa chỉ danh sách bogon.

Bộ lọc black hole, làm giảm lưu lượng truy cập không mong muốn trước khi nó đi vào mạng được bảo vệ. Khi một cuộc tấn công DDoS được phát hiện, máy chủ BGP (Border Gateway Protocol) sẽ gửi các bản cập nhật routing đến các bộ định tuyến router ISP để chúng định tuyến tất cả lưu lượng truy cập đến các server người dùng và sử dụng interface null0 ở bước tiếp theo.

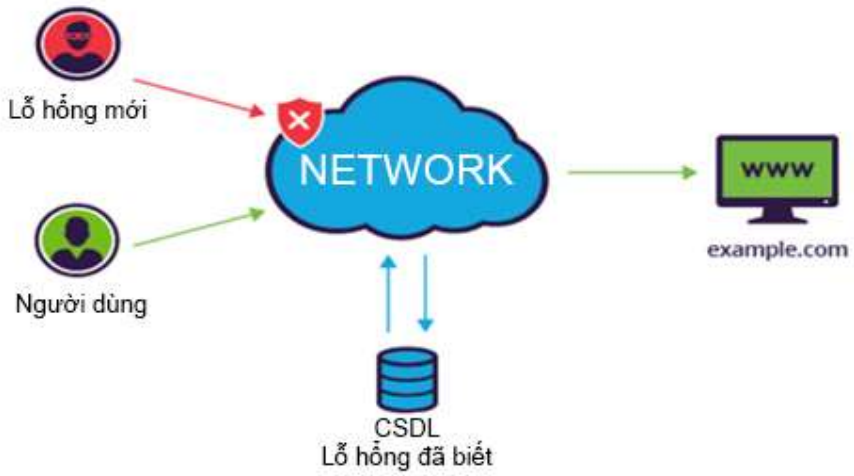
2.2.4. Tấn công cơ sở dữ liệu (SQL injection)

Kẻ tấn công " tiêm " một đoạn mã độc hại vào cơ sở dữ liệu sử dụng ngôn ngữ truy vấn có cấu trúc(SQL), mục đích là khiến máy chủ trả về những thông tin quan trọng mà không được tiết lộ. Các cuộc tấn công SQL injection được xuất phát từ lỗ hổng của website, kẻ tấn công có thể tấn công đơn giản chỉ bằng cách chèn đoạn mã độc vào công cụ Tìm kiếm là đã có thể tấn công website.

Hình 2.7. Tấn công cơ sở dữ liệu

2.2.5. Khai thác lỗ hổng Zero-day (Zero day attack)

Lỗ hổng Zero-day (hay còn gọi là 0-day vulnerabilities) là các lỗ chưa được công bố, các nhà cung cấp phần mềm chưa biết tới do đó chưa có bản vá chính thức. Do đó, việc khai thác các lỗ hổng mới như vậy là cực kỳ nguy hiểm và không thể đoán trước, đồng thời có thể gây ra hậu quả nghiêm trọng cho người dùng và chính nhà xuất bản sản phẩm.



Hình 2.8. Khai thác lỗ hổng Zero-day

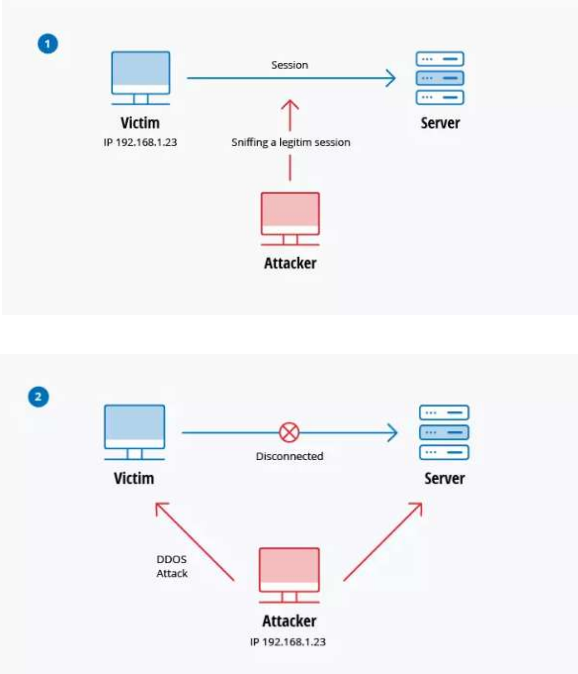
2.2.6. Tấn công Man in the middle (MitM)

Một tấn công MitM xảy ra khi một hacker tự chèn vào giữa các giao tiếp của client và server. Dưới đây là một số kiểu tấn công man-in-the-middle phổ biến:

Session hijacking (chiếm quyền điều khiển)

Trong kiểu tấn công MitM này, hacker chiếm quyền điều khiển một phiên bản giữa client và server mạng đáng tin cậy. Ví dụ, cuộc tấn công có thể diễn ra như thế này:

- Máy client kết nối với server.
- Máy tính của hacker giành được quyền kiểm soát máy client.
- Máy tính của hacker ngắt kết nối máy client khỏi server.
- Hacker thay thế địa chỉ IP của client bằng địa chỉ IP của chính nó và giả mạo sequence number của client.
- Máy tính của hacker tiếp tục trao đổi dữ liệu với server và lúc đó server tin rằng nó vẫn đang giao tiếp với máy client.



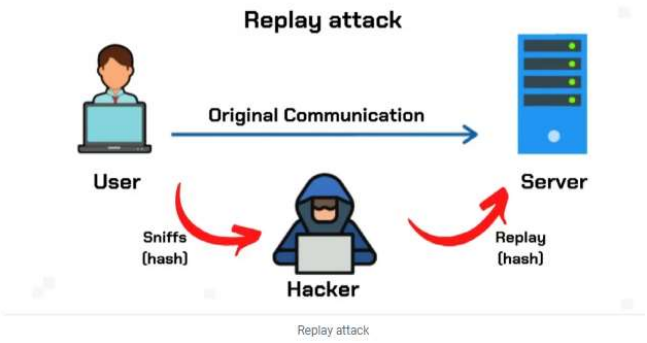
Hình 2.9. Tấn công Man in the middle

Giả mạo IP (IP Spoofing)

Giả mạo IP được hacker sử dụng để thuyết phục hệ thống rằng nó đang giao tiếp với một thực thể (entity) đáng tin cậy, đã biết và cung cấp cho hacker quyền truy cập vào hệ thống. Hacker sẽ gửi một gói với địa chỉ nguồn IP của một server đáng tin cậy, đã biết thay vì địa chỉ nguồn IP của chính nó tới một host mục tiêu. Host mục tiêu có thể chấp nhận gói tin đó và hành động theo nó.

Replay

Một cuộc tấn công phát lại xảy ra khi hacker chặn và lưu các tin nhắn cũ. Sau đó cố gắng gửi chúng đi bằng cách mạo danh một trong những người tham gia. Loại này có thể được đối phó dễ dàng với việc giấu phiên bản thời gian hoặc số nonce (một số ngẫu nhiên hoặc một chuỗi thay đổi theo thời gian).



Hình 2.10. Tấn công Replay

Hiện tại, không có công nghệ hoặc cấu hình duy nhất nào để ngăn chặn tất cả các cuộc tấn công MitM. Nói chung, việc mã hóa và chứng chỉ số SSL sẽ cung cấp biện pháp bảo vệ hiệu quả chống lại các cuộc tấn công MitM, đảm bảo cả tính bí mật và tính toàn vẹn của thông tin liên lạc. Nhưng một cuộc tấn công man-in-the-middle có thể xâm nhập vào giữa các giao tiếp theo cách mà việc mã hóa cũng không giúp ích được gì.

2.2.7. Các loại khác

Ngoài ra, còn có nhiều hình thức tấn công mạng khác như tấn công chuỗi cung ứng, tấn công email, v.v. Mỗi hình thức tấn công đều có những đặc điểm riêng, ngày càng phức tạp và tinh vi buộc các cá nhân, tổ chức phải thường xuyên cảnh giác và luôn cập nhật các công nghệ phòng chống mới.

2.3. Một số giải pháp phòng chống tấn công mạng nội bộ

2.3.1. Sử dụng tường lửa (Firewall)

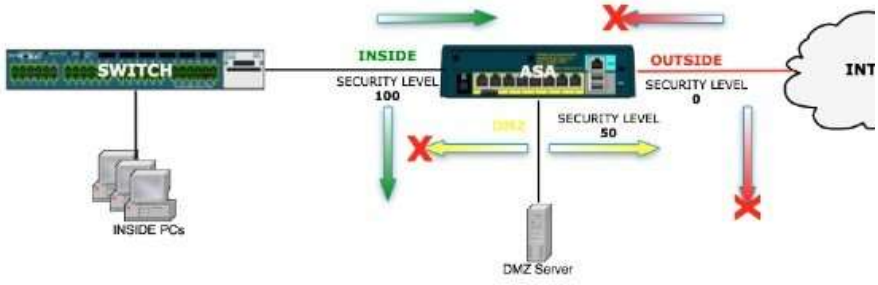
2.3.1.1. Khái niệm

Firewall là thuật ngữ xuất phát từ trong phòng cháy chữa cháy công trình xây dựng, người ta đã thiết kế ra các bức tường có chức năng chống cháy lan, để khi xảy ra hỏa hoạn, lửa sẽ bị chặn lại tại các bức tường có thiết kế đặc biệt này. Thuật ngữ này được áp dụng vào an toàn thông tin, Firewall có tác dụng là một hệ thống phòng thủ, bảo vệ dữ liệu khỏi sự tấn công, và là "chốt chặn", kiểm soát thông tin ra vào hệ thống, hạn chế những truy cập trái phép.

2.3.1.2. Tường lửa cứng

Tường lửa cứng hay Hardware Firewall là thuật ngữ chỉ các thiết bị phần cứng có chức năng kiểm tra tất cả các dữ liệu đi qua và chặn các gói dữ liệu nguy hiểm, hoặc các truy cập không mong muốn. Tường lửa cứng thường được đặt tại phía ngoài của mạng nội bộ, đón dữ liệu từ ngoài trước khi được đưa vào trong mạng nội bộ.

Trong các mạng nhỏ hoặc tại gia đình, các thiết bị định tuyến như Router hoặc Modem cũng được tích hợp tính năng tường lửa và cũng được coi như một thiết bị tường lửa cứng.



Hình 2.11. Mô tả cơ bản vị trí của tường lửa cứng trong mạng

Ưu điểm của tường lửa cứng:

- Tốc độ phản hồi nhanh: có thể xử lý nhiều luồng dữ liệu cùng lúc, phù hợp với mạng có lưu lượng truy cập lớn.
- Bảo mật tốt: tường lửa cứng thường sử dụng hệ điều hành riêng và ít bị tấn công, có thể thiết lập các quy tắc, các chính sách để ngăn chặn tấn công và hạn chế truy cập.
- Linh động: tường lửa cứng là một thành phần trong mạng, nên có thể dễ dàng được quản lý, có thể thay đổi, tắt, hoặc cấu hình lại mà không làm ảnh hưởng đến hoạt động của mạng nội bộ.

Hạn chế của tường lửa cứng:

- Giá thành cao: để trang bị một thiết bị tường lửa cứng chuyên dụng đòi hỏi một khoản kinh phí tương đối lớn, vì vậy chỉ phù hợp với những tổ chức, doanh nghiệp có quy mô lớn.
- Khó để quản trị: tuy bảo mật rất tốt nhưng lại yêu cầu người quản trị có trình độ, để có thể cấu hình, tạo các luật, chính sách cho phù hợp với mạng nội bộ đang sử dụng

2.3.1.3. Tường lửa mềm

Tường lửa mềm là các phần mềm có chức năng kiểm soát truy cập từ bên ngoài, chặn các truy cập trái phép, các mã độc, v.v… Các phần mềm này thường được đóng gói và cài đặt trên hệ điều hành hoặc tích hợp sẵn trên hệ điều hành (ví

dụ như Windows Firewall (Windows Defender) đi kèm hệ điều hành Windows của Microsoft.

Hình 2.12. Phần mềm tường lửa AVS Firewall

Ưu điểm của tường lửa mềm:

- Dễ cài đặt, dễ cấu hình: các phần mềm có tính năng tường lửa trên hệ điều hành đều rất dễ cài đặt, chỉ cần vài thao tác và không đòi hỏi nhiều kỹ năng để có thể sử dụng. Các cấu hình cũng thường được tự động sẵn, có thể tùy chỉnh nếu có chuyên môn
- Chi phí rẻ: tường lửa mềm thường miễn phí. Hầu hết các phần mềm bảo mật hiện nay đều cho cài đặt miễn phí, bản trả phí sẽ có thêm chức năng nhưng cũng không quá đắt, phù hợp với nhu cầu cá nhân và tổ chức doanh nghiệp nhỏ

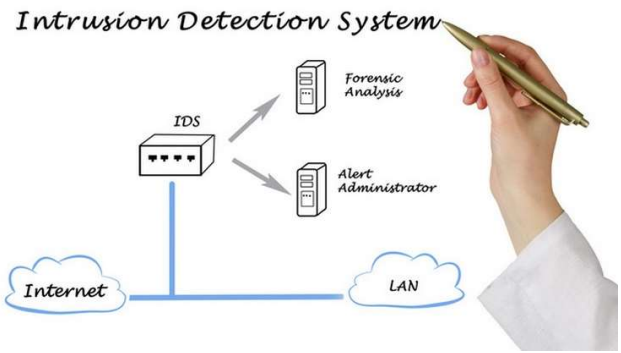
Hạn chế của tường lửa mềm:

- Bảo mật chưa cao: vì là các phần mềm giá rẻ hoặc miễn phí, nên độ bảo mật chưa được cao, vẫn có những lỗ hổng và sẽ phải liên tục cập nhật các bản vá mới nhất để tránh tấn công.
- Linh động: khó hoặc gần như không thể can thiệp sâu vào các quy tắc, chính sách có sẵn.

2.3.2. Công nghệ phát hiện và ngăn chặn xâm nhập IDS/IPS

2.3.2.1. Phát hiện xâm nhập IDS

Hệ thống phát hiện xâm nhập IDS (Intrusion Detection System) là những phần mềm, công cụ có khả năng giám sát mạng, phát hiện những bất thường, các hành vi trái phép, cố gắng xâm nhập vào hệ thống. IDS có thể phát hiện và phân biệt được tấn công từ bên trong (mạng nội bộ) hay từ bên ngoài (từ các hacker lợi dụng lỗ hổng bảo mật).



Hình 2.13. Mô hình diễn tả hệ thống IDS

Hệ thống IDS hoạt động dựa trên các nguy cơ đã biết (từ các cơ sở dữ liệu về bảo mật) hoặc dựa trên sự bất thường khi so sánh lưu lượng mạng.

Chức năng chính của hệ thống IDS:

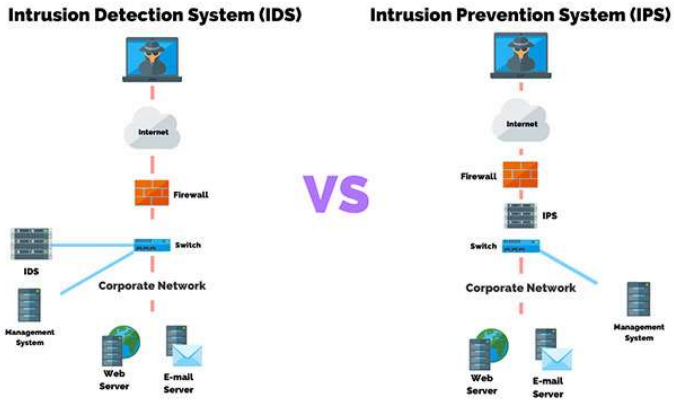
- Giám sát lưu lượng mạng, và các hành vi bất thường.
- Cảnh báo về những tình trạng bất thường cho hệ thống và quản trị viên.
- Kết hợp với các hệ thống giám sát khác, tường lửa, anti-virus, tạo nên một hệ thống bảo mật hoàn chỉnh cho một mạng nội bộ.

2.3.2.2. Ngăn chặn xâm nhập IPS

Hệ thống ngăn chặn xâm nhập IPS (Intrusion Prevention System) là những phần mềm, công cụ có khả năng theo dõi, ngăn chặn kịp thời những hành vi tấn công, xâm nhập mạng nội bộ.

Chức năng chính của hệ thống IPS là xác định các mối nguy cơ, và lưu lại log các thông tin này. Kết hợp với các luật và chính sách của tường lửa để chặn các hoạt động này và đưa ra báo cáo chi tiết.

Hệ thống IPS hoạt động tương tự IDS nhưng ngoài việc giám sát, theo dõi, thì IPS còn chủ động ngăn chặn kịp thời các hành vi gây nguy hiểm cho hệ thống. IPS và IDS có các tập luật, chính sách giống nhau.



Hình 2.14. Sự khác nhau giữa IPS và IDS

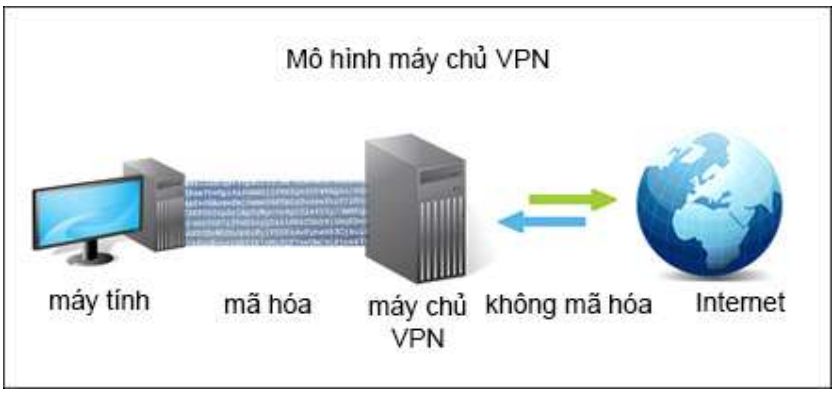
2.3.3. Mạng riêng ảo VPN

Mạng riêng ảo VPN – Virtual Private Network tạo ra các kết nối mạng riêng tư giữa các thiết bị trên môi trường Intranet. VPN được dùng để gửi nhận dữ liệu một cách an toàn và ẩn danh qua các mạng công cộng. Về cơ bản VPN sẽ che dấu địa chỉ IP của người dùng và mã hóa dữ liệu để người được cấp quyền mới có thể sử dụng được.

Ưu điểm của VPN mang lại:

- An toàn: người gửi có thể mã hóa các gói dữ liệu trước khi gửi chúng đi. Bằng việc đó, sẽ hạn chế được những đối tượng xấu truy cập và xem trộm gói tin. Nếu có lấy được gói tin nhưng không giải mã được thì cũng không sử dụng được.

- Tính toàn vẹn của dữ liệu: người nhận có thể kiểm tra xem tập tin mình nhận được so với tập tin được gửi đi có nguyên vẹn hay không, có thay đổi gì trong quá trình gửi hay không.
- Xác thực nguồn gốc: người nhận có thể xác thực được nguồn gốc của các tập tin, đảm bảo đúng người gửi và nguồn thông tin.



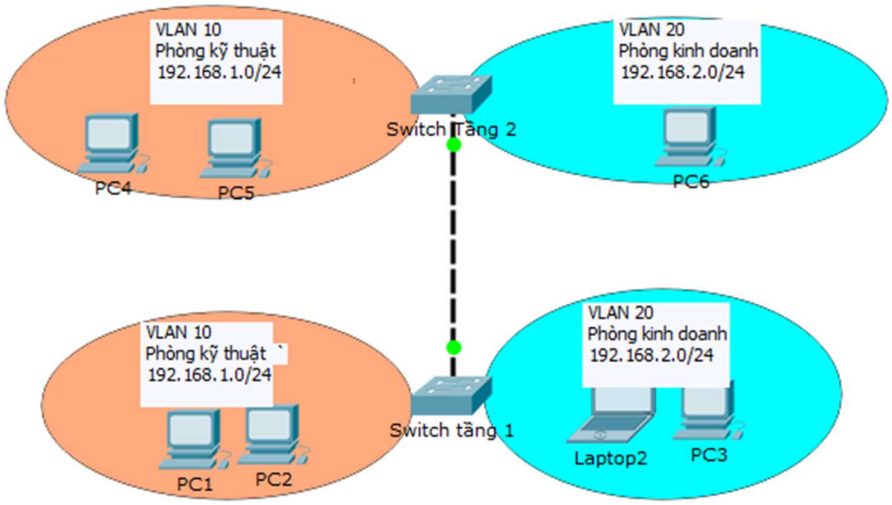
Hình 2.15. Mô hình VPN

2.3.4. Mạng LAN ảo VLAN

Mạng LAN ảo VLAN – Virtual Local Area Network là một nhóm các thiết bị mạng và thiết bị đầu cuối, được gom lại một cách logic, dựa theo các yếu tố đặc trưng như chức năng, bộ phận, vị trí địa lý, ứng dụng…

Lợi ích khi sử dụng VLAN:

- Tiết kiệm băng thông của hệ thống mạng.
- Tăng cường khả năng bảo mật: do có thể tạo các chính sách, tập luật riêng cho từng mạng VLAN. Các thiết bị ở VLAN khác nhau không thể truy cập nhau trừ khi được người quản trị mạng cho phép
- Khả năng mở rộng cao: dễ dàng thêm hoặc loại thiết bị ra vào mạng VLAN



Hình 2.16. Mô hình VLAN trong mạng nội bộ

2.3.5. Các biện pháp khác

Đối với cá nhân:

- Không nên truy cập vào các điểm Wifi công cộng mà không cần mật khẩu
- Không sử dụng phần mềm bẻ khóa (crack) trên mạng
- Bảo vệ mật khẩu cho cá nhân bằng cách đặt mật khẩu phức tạp, bật tính năng bảo mật 2 lớp – xác nhận qua điện thoại,…
- Cập nhật phần mềm, các bản vá lỗi của hệ điều hành lên các phiên bản mới nhất và được nhà sản xuất khuyến nghị.
- Cẩn thận khi nhận E-mail, kiểm tra kỹ tên người gửi, cảnh giác khi click vào link lạ, để phòng tránh mail lừa đảo chuyển hướng người dùng đến các trang giả mạo.
- Không được tải các File không rõ nguồn gốc
- Hạn chế sử dụng các thiết bị ngoại vi như Usb dùng chung.
- Cài đặt phần mềm diệt Virus uy tín.

Đối với tổ chức công ty, doanh nghiệp

- Nghiên cứu và xây dựng các chính sách bảo mật với các điều khoản rõ ràng, chi tiết và minh bạch.
- Lựa chọn kỹ phần mềm và đối tác, ưu tiên những phần mềm có cam kết bảo mật và cập nhật bảo mật thường xuyên, không nên sử dụng phần mềm bẻ khóa trong mạng nội bộ.
- Cập nhật phần mềm, các bản vá bảo mật, Firmware thiết bị lên phiên bản mới nhất được nhà sản xuất khuyến nghị.
- Sử dụng các dịch vụ lưu trữ đám mây uy tín cho mục đích lưu trữ dữ liệu.
- Cần đánh giá bảo mật và xây dựng một chiến lược an ninh mạng tổng thể cho công ty, bao gồm các thành phần: bảo mật cho Website, bảo mật hệ thống máy chủ, mạng nội bộ…
- Thường xuyên tổ chức các buổi huấn luyện, đào tạo, trang bị kiến thức về sử dụng Internet an toàn cho nhân viên.

2.4. Kết luận Chương 2

Trong Chương 2, luận văn đã trình bày một số vấn đề như: tổng quan về an toàn và bảo mật thông tin, một số kỹ thuật tấn công mạng nội bộ phổ biến như: Malware, Phising, DoS và DDoS, SQL injection, Zero-day attack, MitM. Ngoài ra luận văn còn đưa ra một số giải pháp chống tấn công mạn nội bộ như Firewall, IDS/IPS, VPN, VLAN và một số biện pháp liên quan đến yếu tố con người.

Tuy nhiên do số các phương pháp tấn công ngày càng tinh vi và liên tục thay đổi, nên việc phòng chống cũng vì vậy mà gặp nhiều khó khăn do đó cần có sự thử nghiệm và đánh giá.

CHƯƠNG 3: THỰC NGHIỆM VÀ ĐÁNH GIÁ

3.1. Phần mềm hỗ trợ thực nghiệm

3.1.1 Công cụ giả lập EVE-NG

EVE-NG (viết tắt của Emulated Virtual Environment – Next Generation)là một trong các công cụ giả lập (emulator) tốt nhất hiện nay. Cùng các tính năng của UnetLab, Eve-ng có thể giả lập được rất nhiều loại thiết bị mạng đang được sử dụng rộng rãi như router, switch của Cisco (sử dụng Cisco IOL hoặc IOS), thiết bị mạng của Juniper, nhiều loại firewall thông dụng khác như ASA, Pfsense.

Cisco IOL – Cisco IOS on Linux, hoặc một dạng khác là Cisco IOU – Cisco IOS on Unixlà loại IOS chuyên dụng cho việc test tính năng của Cisco được viết để chạy trên nền hệ điều hành Linux (IOL), cho kiến trúc i386 hoặc trên nền hệ điều hành Unix (IOU), cho kiến trúc Sparc. Các hệ điều hành loại này chỉ được sử dụng cho nội bộ của hãng Cisco hoặc cho các khách hàng được ủy quyền và được cấp license. Trong thực tế, hai thuật ngữ IOL và IOU thường được sử dụng hoán đổi với nhau.

Hình 3.1. Công cụ Emulated Virtual Environment – Next Generation

Ưu điểm vượt trội của EVE-NG

- Hỗ trợ thêm giao diện người dùng html5, triển khai thêm các tính năng telnet, vnc, và rpd kết nối trên các thiết bị mà không cần phải mở thêm một TCP port

mới. Điều này cho phép dễ dàng hơn trong việc chạy EVE trên các máy chủ server ở bất kì đâu và cung cấp cơ chế remote để có thể làm việc với nhiều người dùng hơn.

- Các node đã tắt giờ đã được phân biệt các node khác thông qua màu sắc (màu xám cho các node đã tắt thay vì chỉ toàn màu xanh cho mọi node), do đó có thể dễ dàng nhận ra node nào đang chạy và node nào đã tắt.
- UKSM được thực hiện và kích hoạt mặc định, làm giảm thiểu đáng kể bộ nhớ khi so sánh với Unetlab.
- Nhiều loại image được hỗ trợ hơn. Thêm vào đó, ta có thể tìm và lọc ra image khi thêm node mới, điều này thật tuyệt vời bởi vì nếu một list dài các image thì sẽ làm tốn công tìm image mà mình mong muốn.

3.1.2. Hệ điều hành Kali Linux

Kali cung cấp một loạt các tính năng không thể tìm thấy trên các bản phân phối Linux truyền thống:

- Trên 600 công cụ kiểm thử bảo mật hacking, pentest, v.v...
- Các công cụ thu thập thông tin mạng Nmap, Wireshark, v.v...
- Các công cụ tập trung tấn công, khai thác vào Wifi như Aircrack-ng, Kismet và Pixie.
- Đối với các nhu cầu kiểm thử tấn công khai thác vào mật khẩu sẽ có Hydra, Crunch, Hashcat và John the Ripper.
- Có rất nhiều các công cụ hacking được cập nhật liên tục.

Ưu điểm

Tính an toàn: Đội ngũ phát triển của Kali Linux là những cá nhân được tin cậy được cam kết về các gói và sự tương tác với các kho lưu trữ - tất cả được thực hiện bằng nhiều giao thức bảo mật.

Phần hạt nhân của Kali Linux cần được đưa vào các bản sửa lỗi mới nhất để đảm bảo an toàn và được liên tục cập nhật để đề phòng nhiễm virus.

Hệ thống mã nguồn mở và miễn phí: Linux luôn phát triển theo mô hình mã nguồn mở nên Kali Linux luôn được miễn phí, và tất nhiên tất cả các mã nguồn của Kali Linux cũng là mã nguồn mở, tất cả mọi người có thể tuỳ chỉnh và thay đổi theo nhu cầu.

Hình 3.2. Hệ điều hành cung cấp các công cụ kiểm thử tấn công Kali Linux

Ưu điểm về phần mềm và phần cứng: Kali có thể sử dụng các repository của Debian hỗ trợ việc cài đặt được nhiều phần mềm và cập nhật phần mềm nhanh chóng

Kali Linux liên tục cải tiến khả năng tương thích với thiết bị phần cứng của rất nhiều loại như điện thoại, raspberry, laptop, server, cloud, v.v... có thể cài đặt trên bất kì thiết bị nào

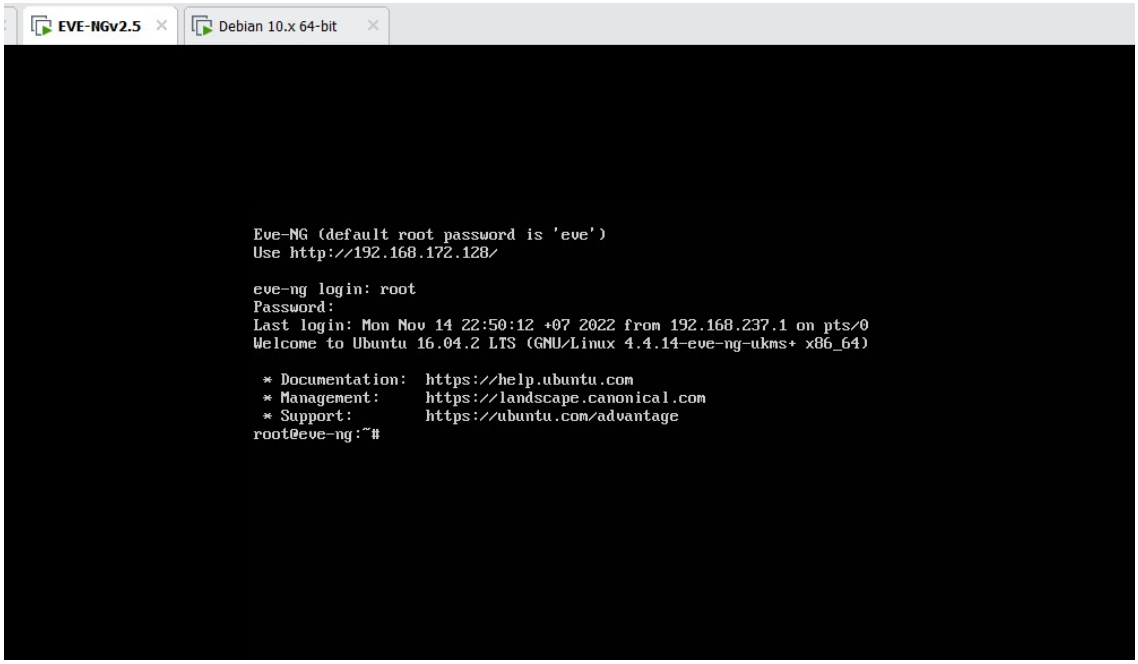
Ưu điểm về kết nối mạng wifi và thiết bị không dây: Kali Lunux hỗ trợ rất tốt cho mạng wifi (không dây), điều này giúp các chuyên gia bảo mật có thể thực hiện tấn công và kiểm thử khả năng bảo mật của Wifi.

Kali Linux được cải tiến để hỗ trợ nhiều thiết bị không dây nhất có thể, cho phép nó hoạt động tốt trên nhiều loại phần cứng và làm cho nó tương thích với nhiều thiết bị không dây và USB khác nhau.

Số lượng phần mềm hỗ trợ hạn chế, không đa dạng và thông dụng như các hệ điều hành khác.

3.2. Cài đặt và triển khai mô hình

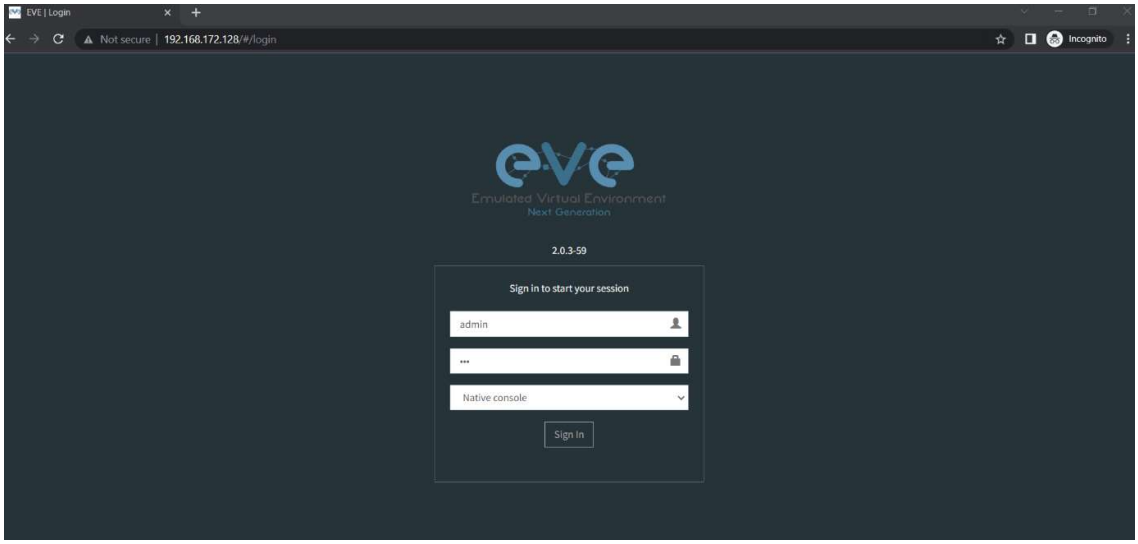
- Tải và cài đặt máy ảo Eve-Ng trên Vmware
- Màn hình sau khi đăng nhập vào eve với user: **root** và password: **eve**



Hình 3.3. Cài đặt Eve-ng trên VMware

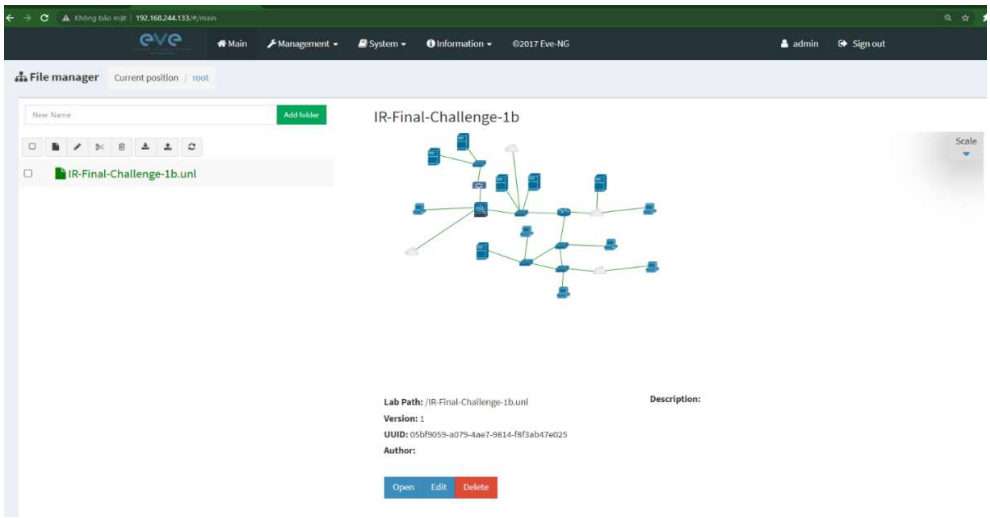
- Truy cập http://IP_Eve/ bằng trình duyệt đăng nhập vào eve bằng

  Username: **admin** và password : **eve.**



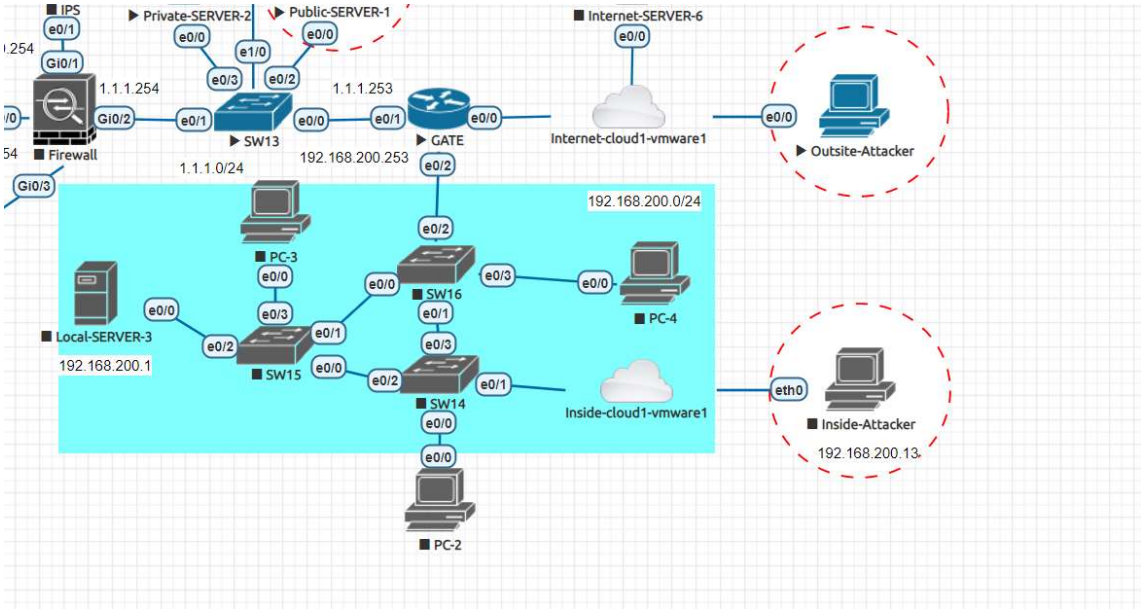
Hình 3.4. Đăng nhập tài khoản sử dụng Eve-ng

- Sau khi đăng nhập vào Eve, import file Lab đã dựng sẵn:



Hình 3.5. Import sơ đồ lab đã tạo

Mô hình mạng được sử dụng trong demo:



Hình 3.6. Mô hình thử nghiệm

3.3. Kịch bản thử nghiệm

Như đã trình bày tại Chương 2, hiện nay có rất nhiều hình thức tấn công mạng nội bộ, các hình thức tấn công rất tinh vi và luôn thay đổi. Tuy nhiên trong phạm vi luận văn, học viên chỉ có thể thực nghiệm được một số phương pháp tấn công, bao gồm:

Tấn công từ trong mạng nội bộ:

- ✓ MAC-Overflow: Máy attacker sẽ nằm cùng mạng nội bộ với máy nạn nhân sau đó thực hiện tấn công DoS thiết bị Switch mà 2 máy đang nối dẫn đến Switch bị sập nguồn, reset ảnh hưởng đến hệ thống mạng.
- ✓ ARP- Poisoning: Kẻ tấn công sẽ giả mạo và từ đó đánh cắp thông tin dữ liệu trong nội bộ khi các PC nạn nhân giao tiếp trong mạng nội bộ.

Tấn công từ bên ngoài vào hệ thống:

- ✓ Access-Cracking: Máy attacker ở bên ngoài outside sử dụng các công cụ scan như nmap để dò ra được địa chỉ IP public của công ty từ đó do thám được thông tin của thiết bị và nghiên cứu lỗ hổng để tấn công vào vùng biên. Sau đó sử dụng công cụ Hydra để bẻ khóa mật khẩu xâm nhập vào hệ thống.

Cả 3 phương pháp tấn công trên đều sử dụng chung một bài Lab, một mô hình mạng để thực nghiệm (hình 3.6)

3.3. Tiến hành tấn công và phòng thủ trên mô hình thử nghiệm

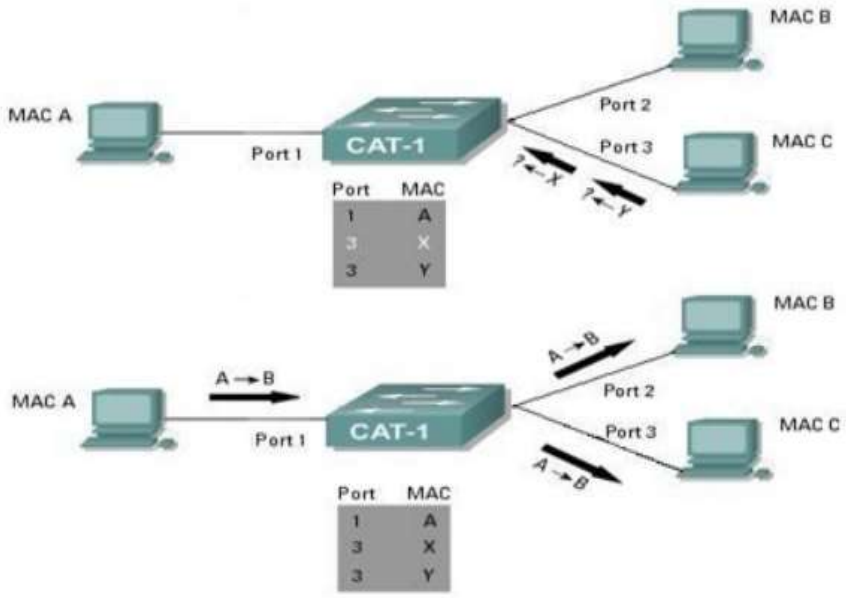
3.3.1. Kỹ thuật tấn công MAC-Overflow

3.3.1.1. Tổng quan về tấn công làm tràn bảng MAC

Tấn công làm tràn bản MAC là một dạng tấn công từ chối dịch vụ (DoS) với mục đích chính là làm tràn bộ nhớ MAC dẫn đến thiết bị hoạt động không chính xác hoặc gây gián đoạn kết nối trong mạng nội bộ.

Tấn công làm tràn bảng MAC dựa vào điểm yếu của thiết bị chuyển mạch cụ thể là thiết bị Switch: bảng MAC chỉ có thể chứa được một số hữu hạn các ánh xạ (như switch Catalyst 6000 có thể chứa tối đa là 128.000 ánh xạ) và các ánh xạ này không phải tồn tại mãi trong bảng MAC. Sau một khoảng thời gian nào đó thường là 300 s nếu địa chỉ này không được dùng trong việc trao đổi thông tin thì nó sẽ bị gỡ bỏ. Khi bảng MAC được điền, tất cả thông tin đến sẽ được gửi đến tất cả các cổng của nó ngoại trừ cổng mà nó nhận được, vì vậy chức năng chuyển mạch không khác gì chức năng của một thiết bị hub.

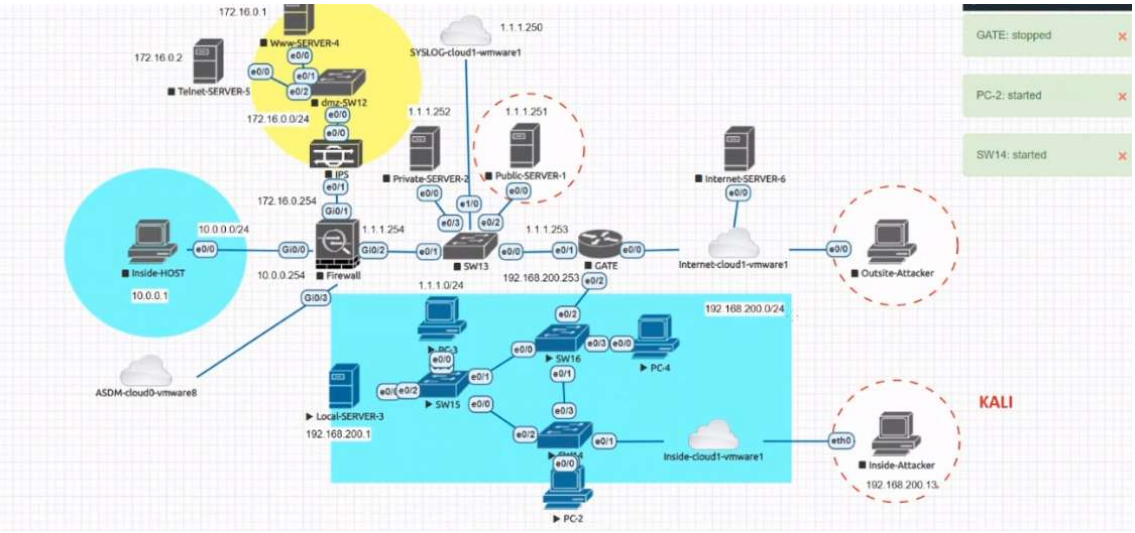
Hình minh họa dưới ta thấy host C của attacker gửi liên tục hàng loạt các bản tin có địa chỉ MAC giả mạo là host X và host Y. Từ đó switch sẽ cập nhật địa chỉ của các host giả mạo này vào bảng MAC. Kết quả là từ host A gửi tin đến cho host B thì địa chỉ của B không tồn tại trong bảng nên gói tin được switch gửi ra các cổng của nó và bản tin A chỉ gửi riêng cho B cũng sẽ được chuyển qua C.



Hình 3.7. Minh họa bảng MAC

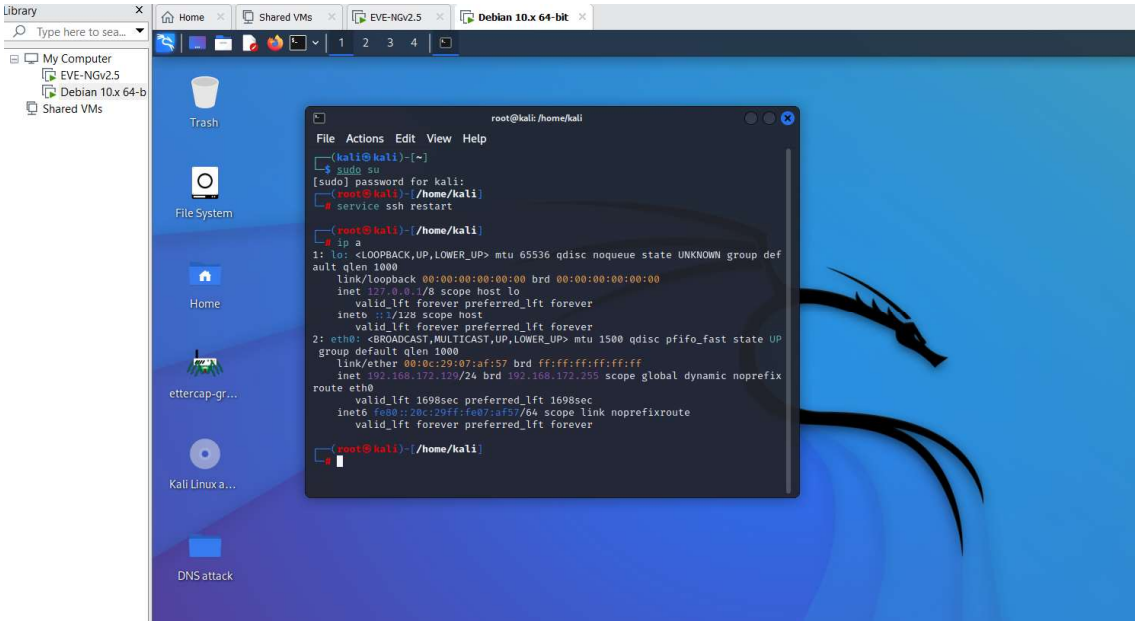
3.3.1.2. Phương thức tấn công MAC-Overflow

Attacker nằm bên trong sau khi đã chiếm quyền hoặc nhân viên đã bị mua chuộc, gián điệp trực tiếp tấn công từ bên trong vùng inside:



Hình 3.8. Sơ đồ tổng quan kịch bản MAC Overflow trên Eve-ng

Mở máy ảo Kali linux:

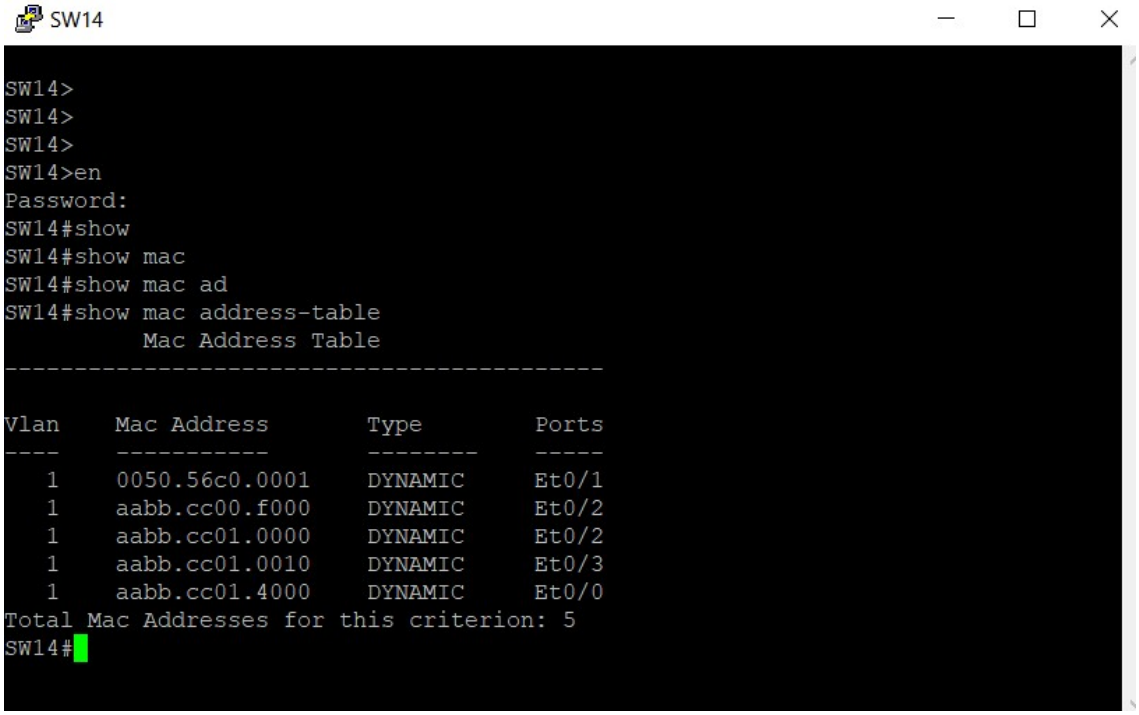


Hình 3.9. Mở máy ảo Kali linux

Mục tiêu tấn công MAC size của thiết bị switch:

- Gửi liên tục MAC giả mạo khiến treo switch
- Switch cũng sẽ bị tấn công từ chối dịch vụ
- Bản MAC bị điền đầy nên full dẫn đến các MAC PC hợp lệ không đặt được ở bảng nữa -> Swịch sẽ hoạt động kiểu flooding (các PC trao đổi dữ liệu với nhau thay vì truyền đúng cổng thì nó chuyển đến các cổng vì không tìm MAC các PC kia do hết chỗ) nên attacker có thể nghe lén.

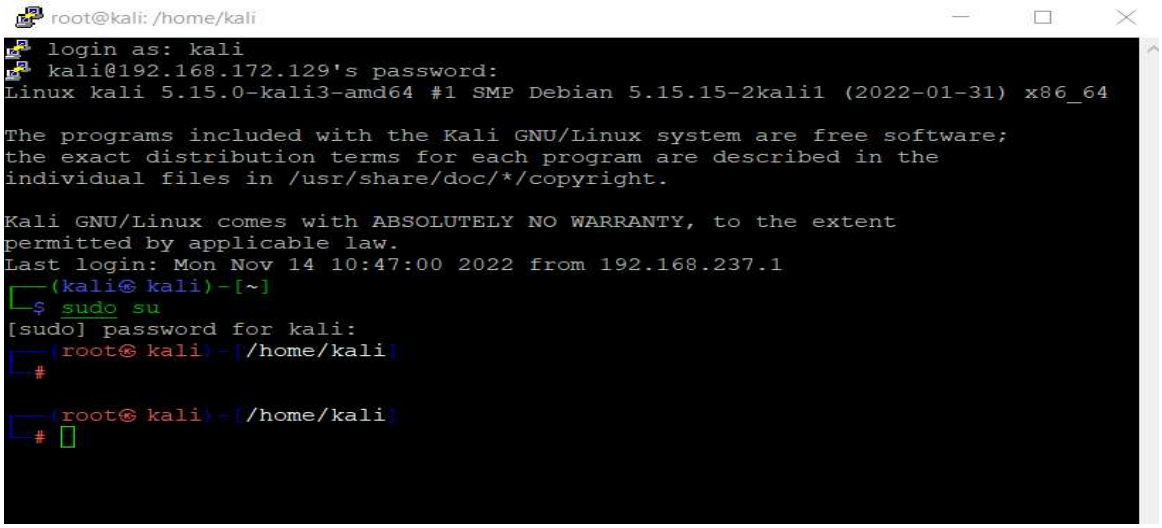
Bảng MAC trước khi bị tấn công:



Hình 3.10. Hiển thị bảng MAC thiết bị SW14 ban đầu

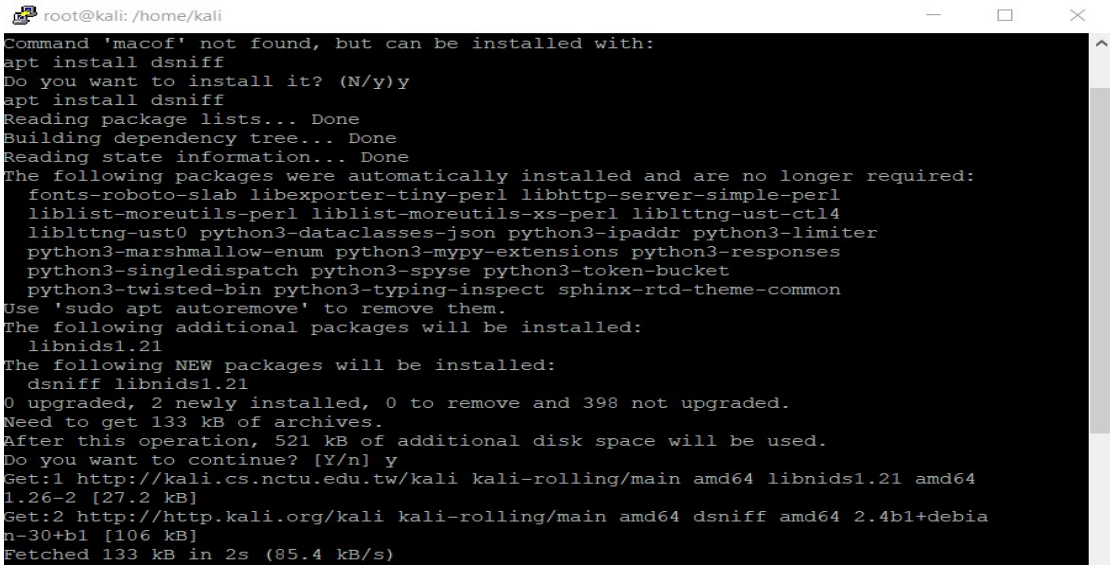
Truy cập terminal máy Kali:

✓ Mở terminal Kali:



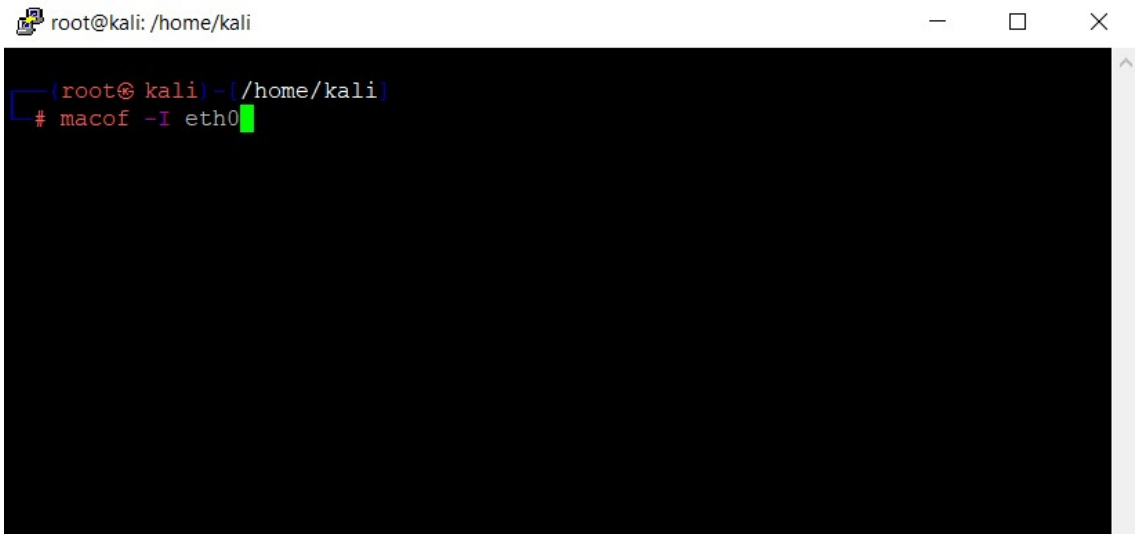
Hình 3.11. Mở terminal máy kali linux

✓ Cài đặt gói dnsiff



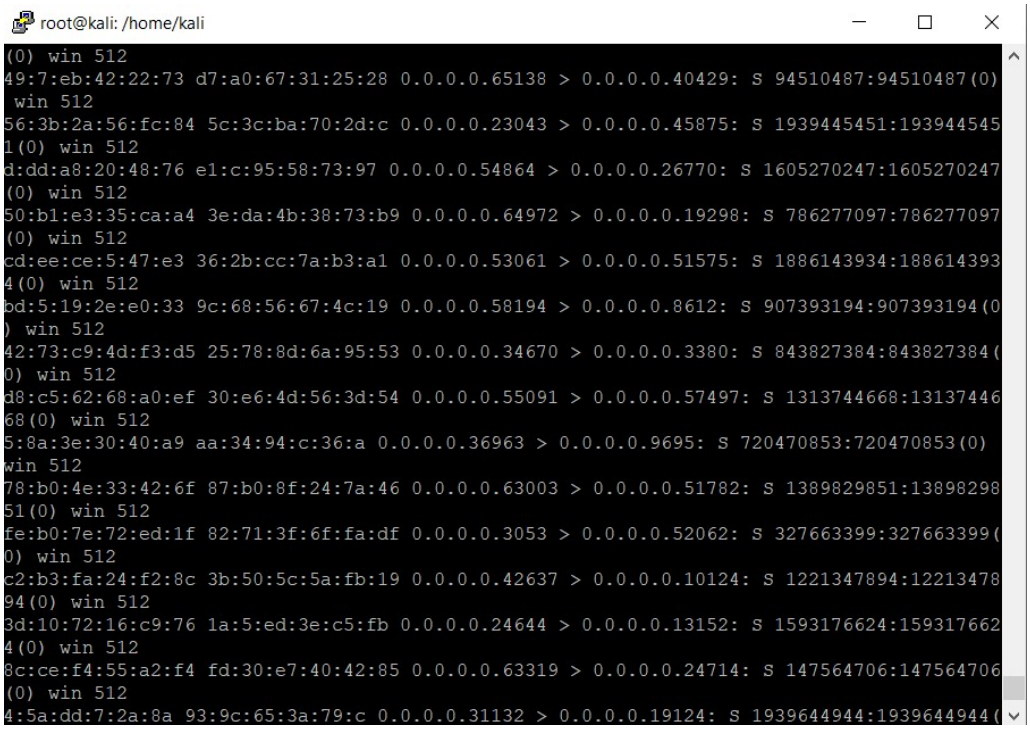
Hình 3.12. Cài đặt gói dnsiff

- Sử dụng câu lệnh macof –I eth0



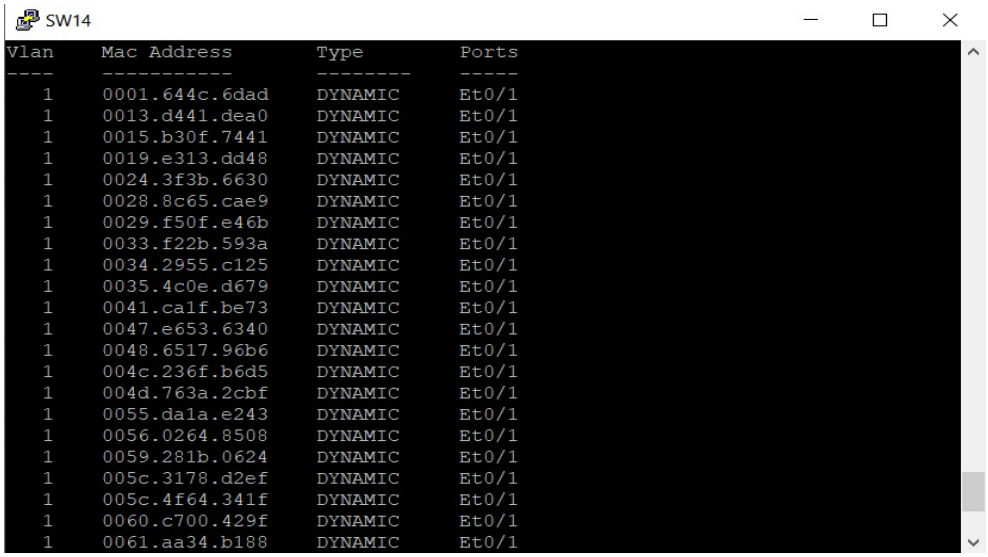
Hình 3.13. Sử dụng lệnh DoS thiết bị SW14

Xuất hiện các MAC giả mạo được Kali gửi liên tục:



Hình 3.14. Máy attacker gửi liên tục các địa chỉ MAC giả mạo

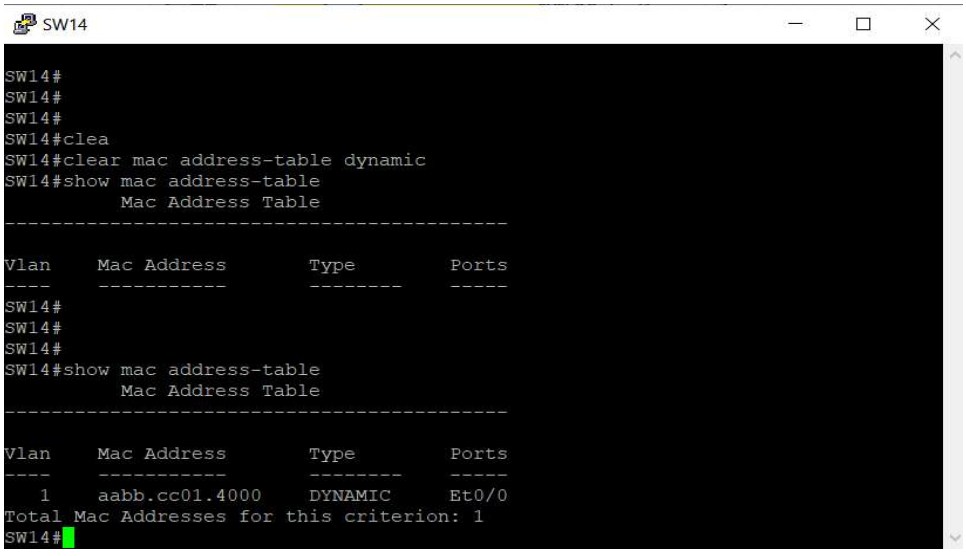
Bên SW4 ta chạy lại câu lệnh show mac table để xem MAC address từ các cổng:



Hình 3.15. Hiển thị bảng MAC trên SW14 sau khi bị attack

Ta thấy xuất hiện rất nhiều MAC giả mạo traffic từ cổng E0/1:

- Sử dụng câu lệnh clear để xoá các MAC giả mạo



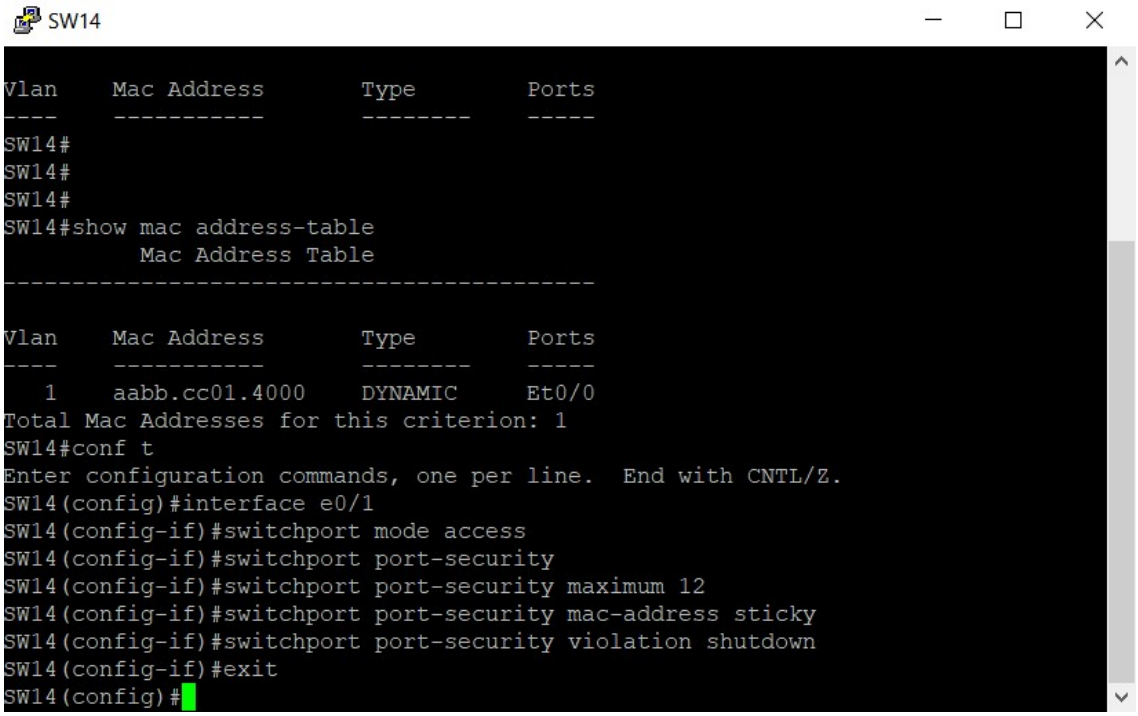
Hình 3.16. Clear bảng MAC trên SW14

3.3.1.3 Giải pháp phòng vệ

Giải pháp ta sử dụng port security bằng câu lệnh cho SW4 :

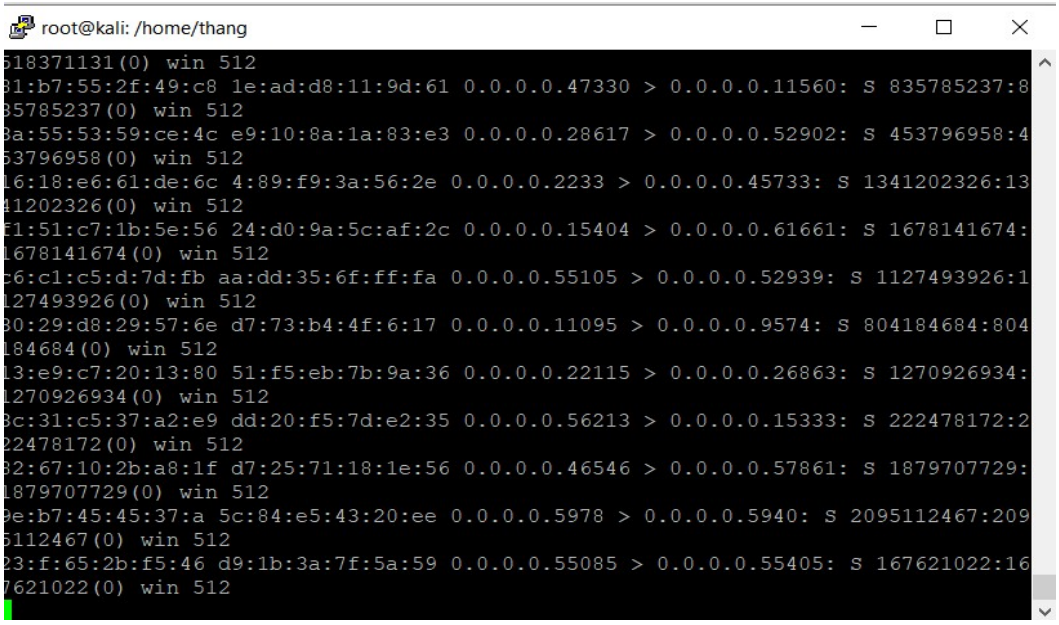
- interface e0/1
- switchport mode access
- switchport port-security
- switchport port-security maximum 12
- switchport port-security mac-address sticky
- switchport port-security violation shutdown

Giải pháp port security trên một cổng này chỉ cho 1 số lượng MAC nhất định nào đó để kết nối vào và nếu có nhiều MAC gửi kết nối và sẽ shutdown cổng:



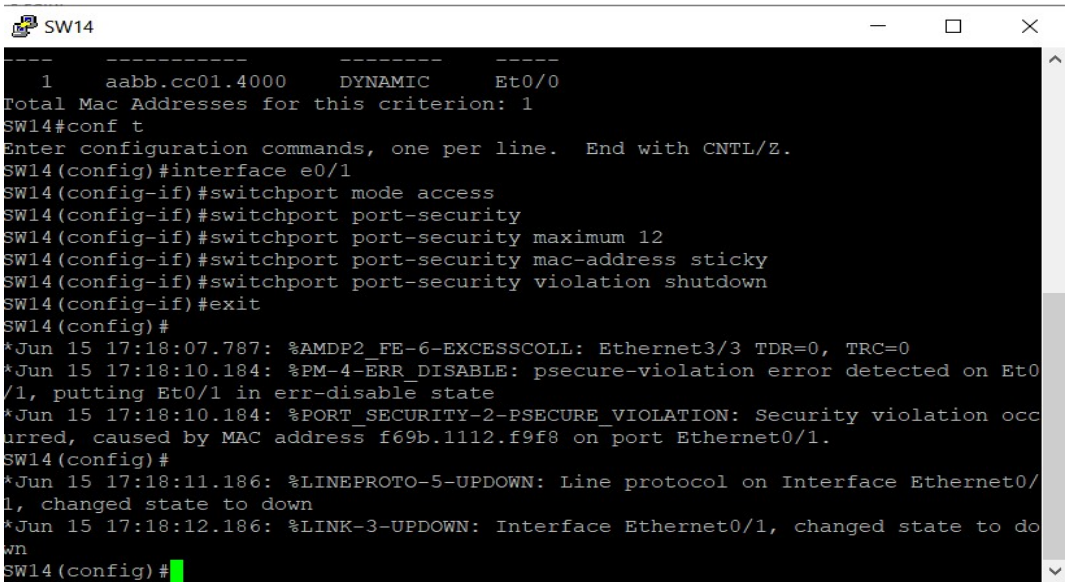
Hình 3.17. Cấu hình port security trên SW14

Sau đó bên kali ta gửi lại MAC địa chỉ giả mạo lần nữa:



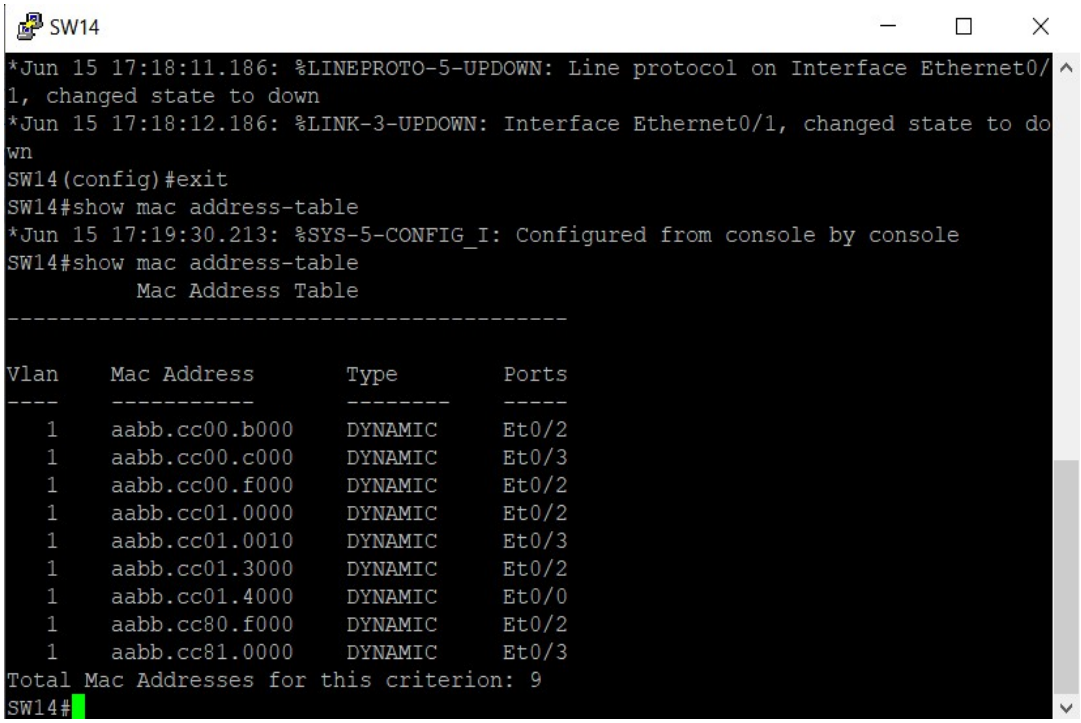
Hình 3.18. Từ máy attacker tấn công lại lần 2

Sau đó kiểm tra thấy cổng E 0/1 cua SW4 đã shutdown sau khi nhận quá nhiều địa chỉ MAC giả mạo:



Hình 3.19. Cổng Ether0/1 của Sw14 tự động ngắt khi thấy dấu hiệu attack

Kiểm tra lại địa chỉ MAC thấy không có thay đổi bất thường.



Hình 3.20. Kiểm tra lại bảng MAC của thiết bị SW14 thấy bình thường

Kiểu tấn công này có 2 hậu quả:

Do quá nhiều traffic điền đầy bảng MAC tiêu tốn nhiều ô nhớ RAM (treo switch), nếu trên hệ thống thật cũng có thể xảy ra (dấu hiệu là đèn trên thiết bị switch nhấp nháy liên tục và nó sẽ tự restart do cạn kiệt tài nguyên).

Do đầy bảng MAC nhiều PC hợp lệ kết nối với nhau và khi trao đổi data với nhau thì switch sẽ flooding.

3.3.2. Kỹ thuật tấn công ARP-Poisoning

3.3.2.1. Lỗ hổng của ARP

ARP (viết tắt của Address Resolution Protocol) là một giao thức truyền thông được sử dụng phổ biến để tìm ra các địa chỉ tầng liên kết dữ liệu từ các địa chỉ mạng.

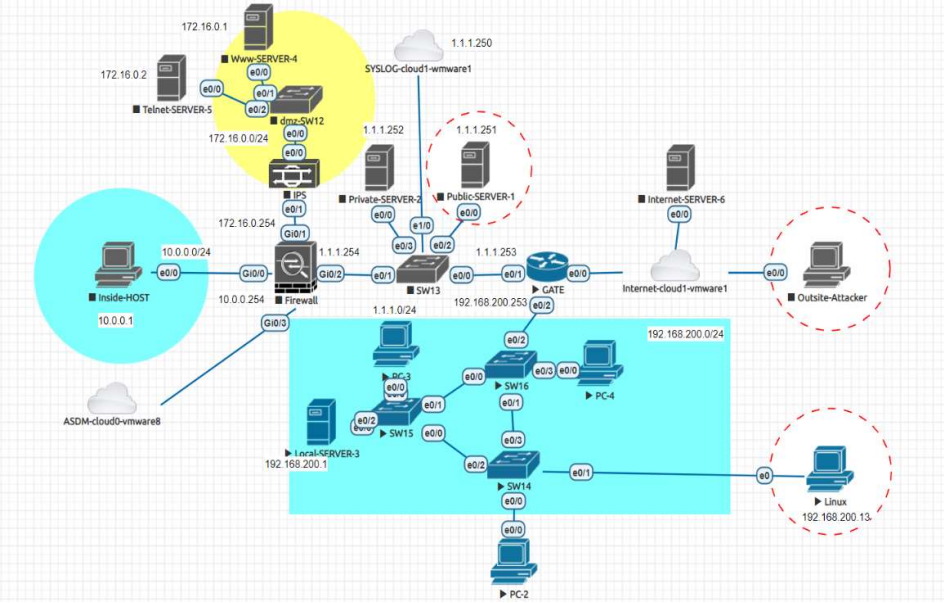
Khi đó một gói tin được gửi từ một máy đến máy khác trong mạng nội bộ thì địa chỉ IP dích phải được giải quyết thành địa chỉ MAC đến truyền qua tầng liên kết dữ liệu. Sau đó khi biết được địa chỉ IP của máy đích và địa chỉ MAC của nó cần truy cập, một gói tin là broadcast được gửi đi trên mạng nội bộ. Gói này được gọi là ARP request. Máy destionation với IP trong ARP request sẽ trả lời với thông tin ARP reply, nó chứa một địa chỉ MAC cho IP đó ARP là một giao thức phi trạng thái.

Máy chủ trong mạng sẽ tự động lưu trữ bất kì ARP reply nào mà chúng có thể nhận được, bất kể máy khác có yêu cầu hay không. Và ngay cả các ARP chưa hết hạn sẽ bị ghi đè khi nhận được gói tin ARP reply mới. Do đó không có phương pháp nào trong giao thức ARP giúp một máy có thể xác nhận máy mà từ đó gói tin bắt nguồn. Cơ chế hoạt động này chính là lỗ hổng cho phép ARP spoofing xảy ra.

3.3.2.2. Phương thức tấn công ARP-Poisoning

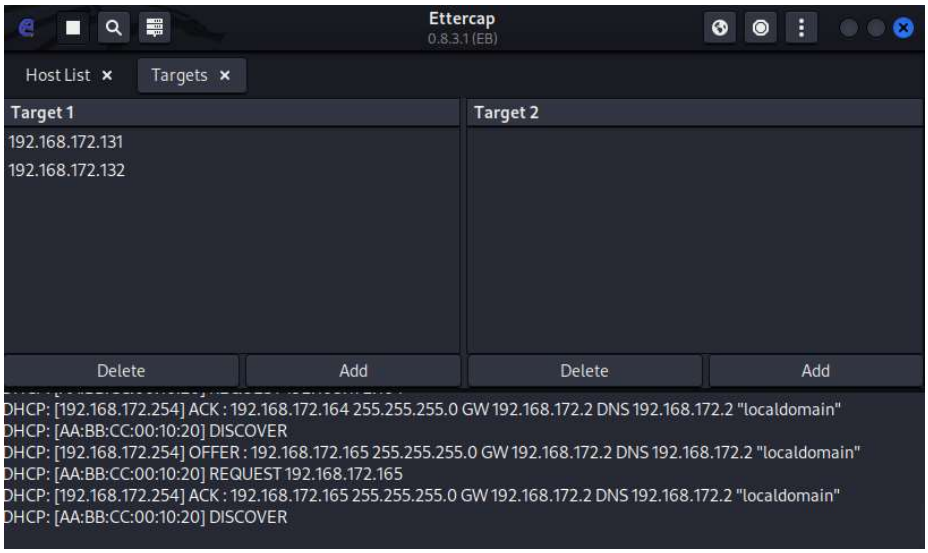
Trong hệ thống mạng, ARP spoofing hay ARP poisoning, ARP poisoning routing là một kỹ thuật thông qua đó kẻ tấn công giả mạo thông điệp ARP trong mạng cục bộ. Mục tiêu sẽ là kết hợp địa chỉ MAC của kẻ tấn công cùng với địa chỉ IP của máy khác, như cổng mặc định (default gateway) làm cho bất kì lưu lượng truy cập nào dành cho địa chỉ IP đó được gửi đến kẻ tấn công ARP spoofing.

Điều này cho phép kẻ tấn công chặn các khung dữ liệu trên mạng, sửa đổi lưu lượng hoặc dừng tất cả lưu lượng. Thường cuộc tấn công này được sử dụng như một mở đầu cho các cuộc tấn công khác, chẳng hạn như tấn công từ chối dịch vụ hoặc các cuộc tấn công đánh cắp dữ liệu. ARP Poisoning là một dạng tấn công Man in the Middle.



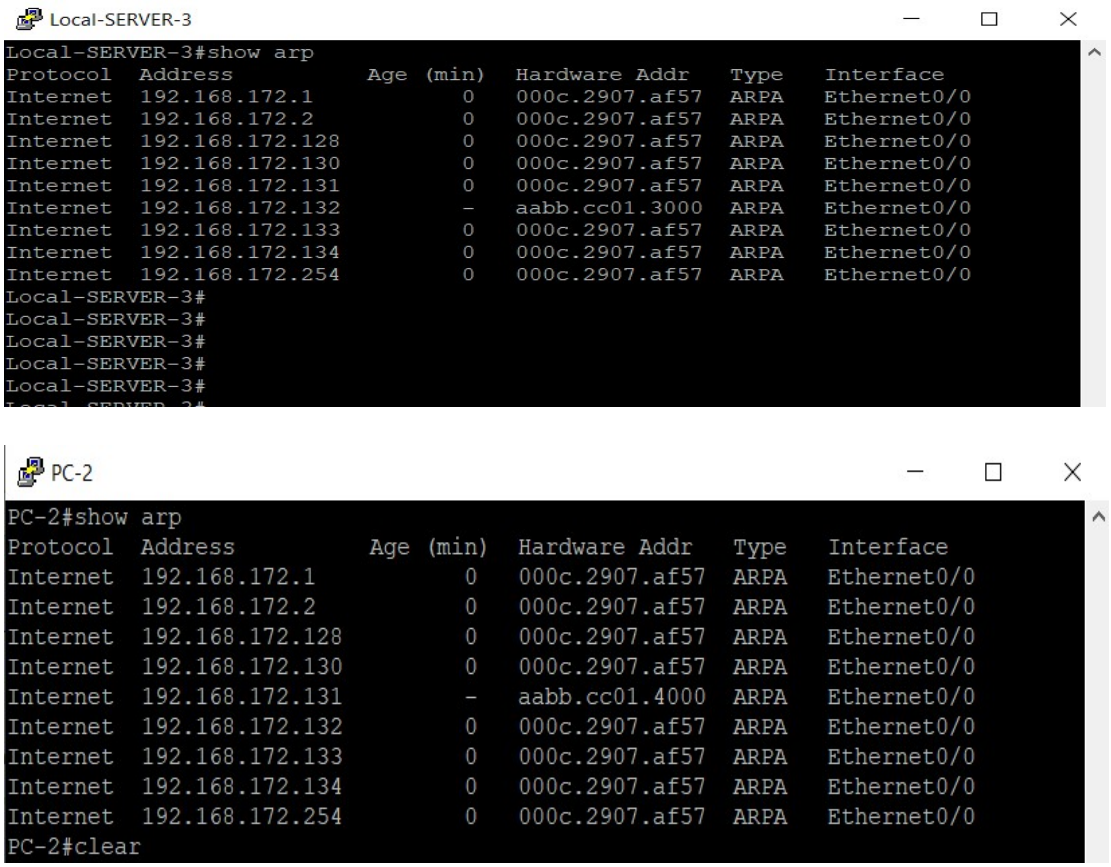
Hình 3.21. Sơ đồ bài lab tấn công ARP-Poisoning

Theo sơ đồ trên ta tập trung cho 2 thiết bị là PC-2, Local-Server-3 và thiết bị GATE đóng vai trò là máy chủ DHCP cấp phát ip lần lượt là Local-SERVER-3: 192.168.172.131 và PC-2: 192.168.172.132. Tiếp theo từ máy Kali ta thực hiện tấn công ARP-Poisoning với công cụ Ettercap:



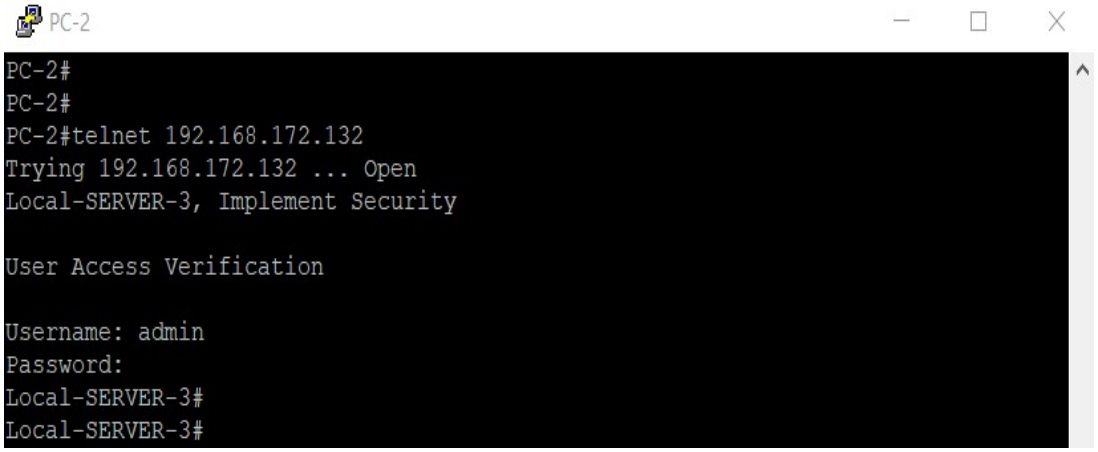
Hình 3.22. Trên máy attacker add 2 mục tiêu PC2 và Local Server3

Sau khi thực hiện tấn công, ta xem thông tin arp của 2 thiết bị nạn nhân đều thấy các thiết bị cùng 1 địa chỉ MAC, ở đây chính là địa chỉ MAC của máy Kali:



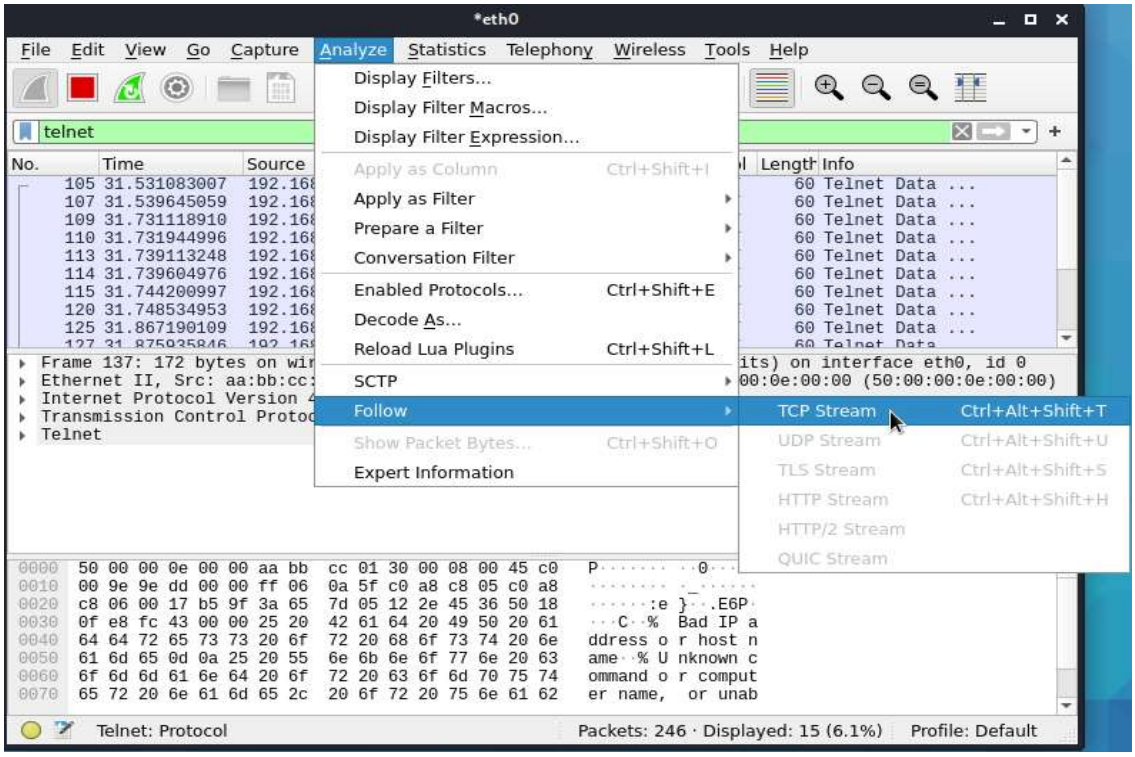
Hình 3.23. Kiểm tra bảng MAC của các thiết bị nạn nhân

Sau đó thực hiện máy PC-2 telnet đến máy Local-Server-3:



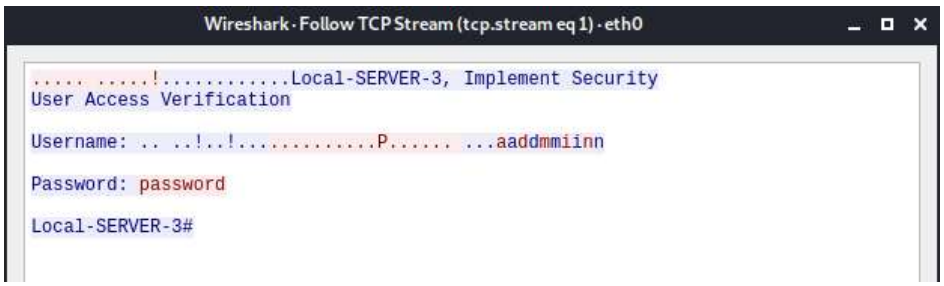
Hình 3.24. Thực hiện từ máy PC2 telnet đến Local Server 3

Từ đây máy kali có thể thực hiện nghe lén tài khoản và mật khẩu sử dụng công cụ WireShark:



Hình 3.25. Máy attacker sử dụng công cụ Wireshark để nghe lén

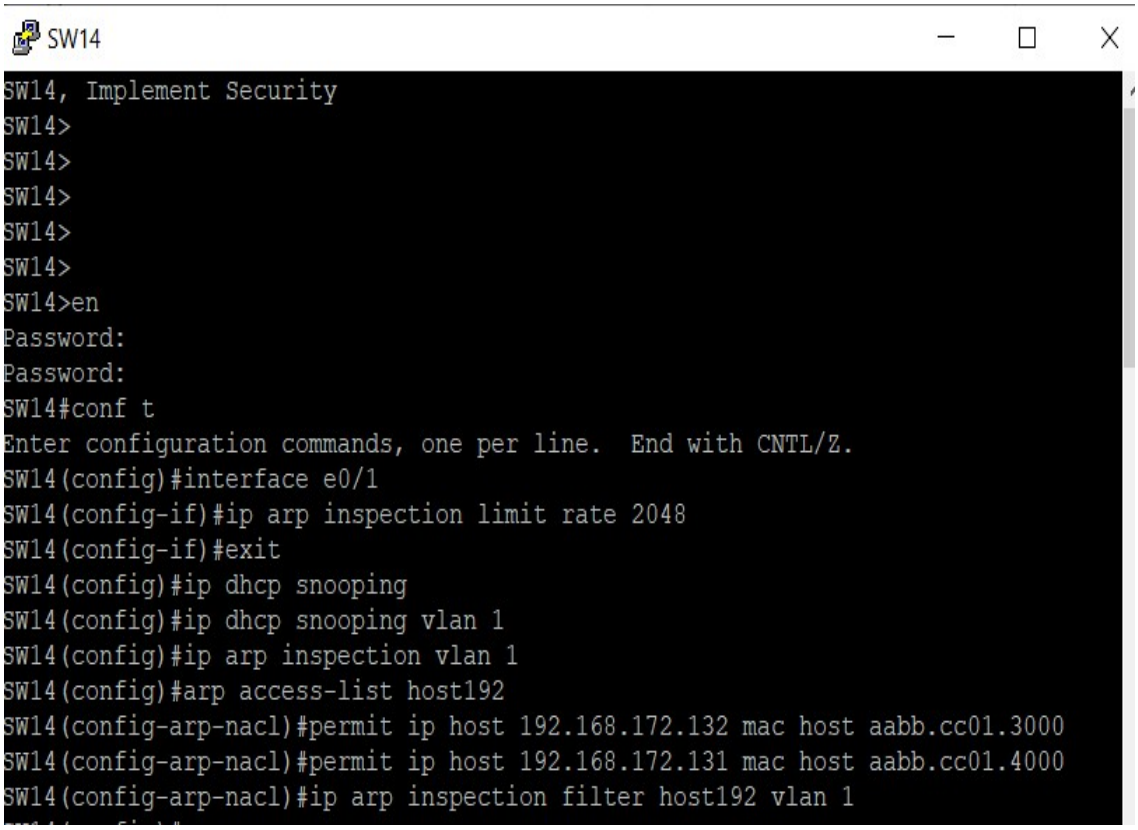
Ta có thể thấy hiện tài khoản và mật khẩu để telnet đến Local-Server-3:



Hình 3.26. Attacker dò được tài khoản telnet

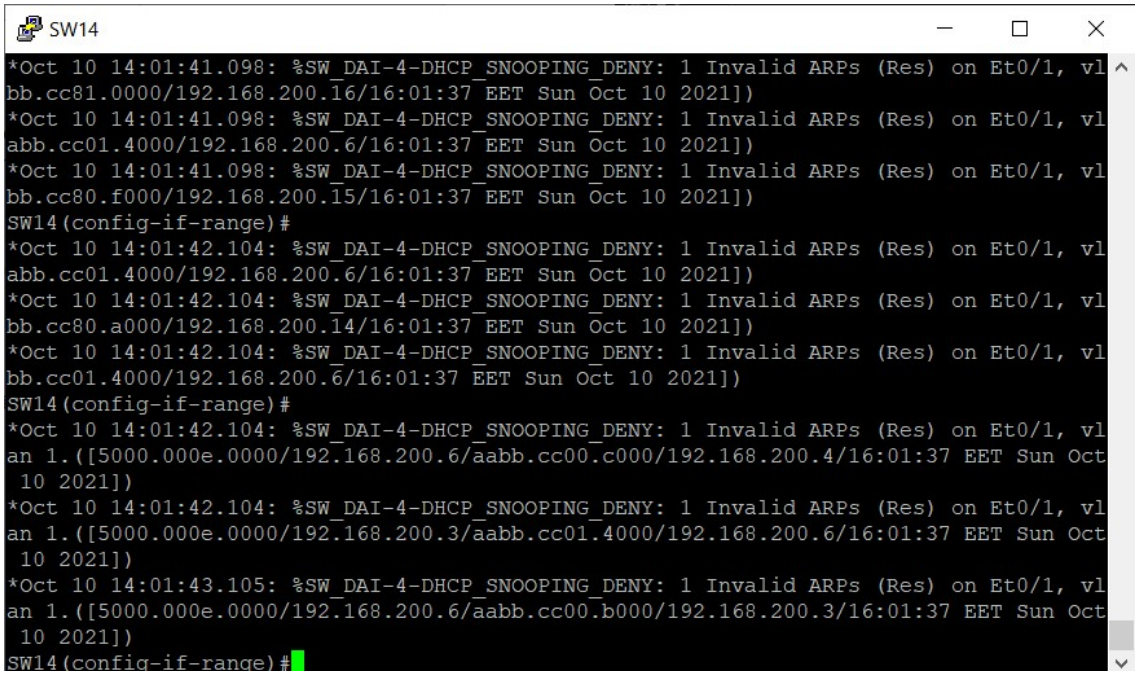
3.3.2.3. Giải pháp

Giải pháp ở đây là ta sử dụng ip snooping trên Switch14 với mục đích là chặn các gói arp giả mạo của kẻ tấn công. Cấu hình trên SW14 như sau:



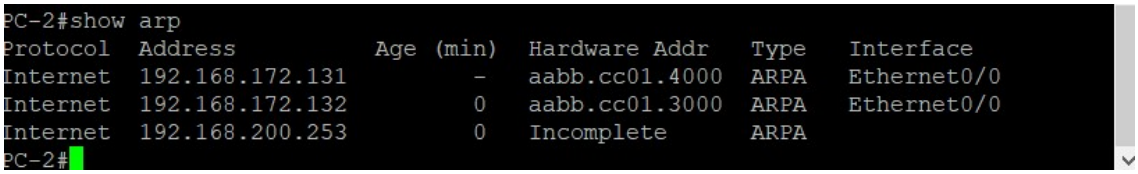
Hình 3.27. Cấu hình ip snooping trên SW14 để phòng vệ

Sau khi cấu hình máy kali thực hiện tấn công lại sẽ xuất hiện các dòng thông báo chặn gói ARP của cổng e0/1 SW14:

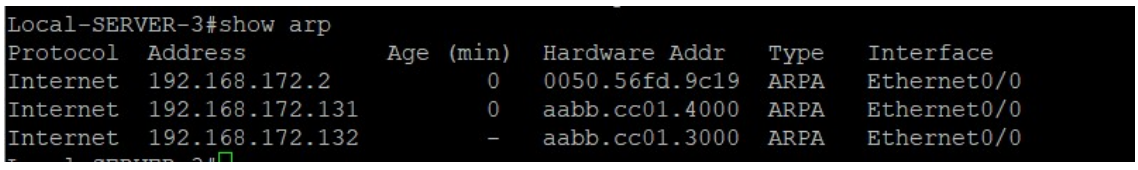


Hình 3.28. Tấn công lại lần nữa từ máy Attacker thấy SW14 hiện cảnh báo

Và địa chỉ MAC của 2 thiết bị PC-2 và Local-SERVER-3 không bị thay đổi



Hình 3.29. Kiểm tra lại bảng Mac của thiết bị PC2 thấy bình thường



Hình 3.30. Kiểm tra lại bảng Mac của thiết bị Local-Server3 thấy bình thường

3.3.3. Phương thức tấn công Access-Cracking

Việc hệ thống mục tiêu sử dụng các cấu hình được thiết lập mặc định bởi nhà sản xuất thiết bị phần cứng hay phần mềm làm cho việc tấn công vào mục tiêu đó trở nên dễ dàng hơn bao giờ hết.

Nhiều công cụ tấn công và các mã khai thác giả định rằng mục tiêu đang sử dụng các thiết lập mặc định (default setting). Vì vậy, một trong các phương án phòng ngừa hiệu quả và không thể bỏ qua là đơn giản thay đổi các thiết lập mặc định này.

Các rất nhiều dạng thiết lập mặc định như: username, password, access code, path name, folder name, component, service, configuration, setting… Nhiệm vụ của ta là cần biết tất cả các thiết lập mặc định của các sản phẩm phần cứng và phần mềm mà mình đã hoặc sắp triển khai và cố gắng thay đổi các thiết lập mặc định đó thành các thiết lập khác bí mật hơn. Ta có thể xem trong tài liệu đi kèm với sản phẩm và dịch vụ hoặc tìm kiếm trên Internet để biết được hệ thống của mình có những thiết lập mặc định nào.

Ví dụ sau: thiết lập mặc định cho phép hacker có thể truy cập và quản lý router giả sử có tên model là ABC-123 của nạn nhân từ xa có thể thông qua HTTP, Telnet, SSH… là username và password mặc định của tài khoản có quyền quản trị. Hacker có thể tìm kiếm trên Internet với từ khóa “default password + ABC-123” là có thể dễ dàng biết được thiết lập mặc định mà một số người dùng thường quên đổi đi này.

Giải pháp là điều chỉnh lại các lựa chọn mặc định khi có thể như:

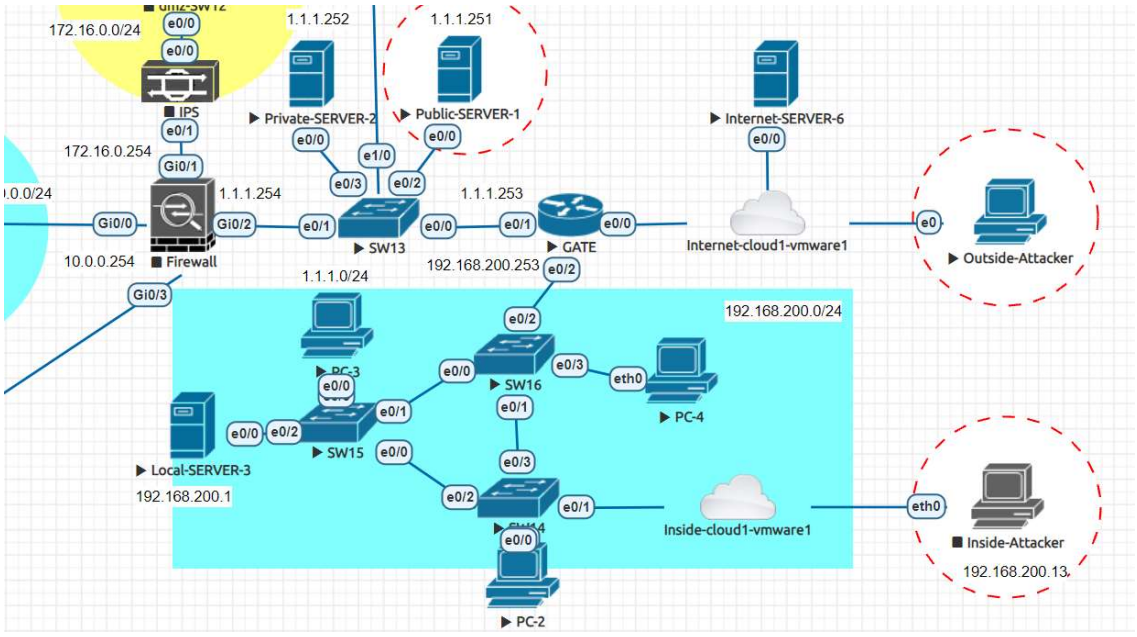
– Cố gắng tránh cài đặt hệ điều hành lên các ổ đĩa và thư mục mặc định.

– Đừng cài đặt các ứng dụng, phần mềm tới các vị trí chuẩn của chúng…

Ta điều chỉnh càng nhiều các thiết lập mặc định thì hệ thống của mình sẽ trở nên ‘khó tương thích’ hơn với các công cụ và mã khai thác của hacker, đồng nghĩa với việc hacker cần nhiều nỗ lực hơn để tấn công vào mục tiêu.

3.3.3.1. Tấn công Access-Cracking

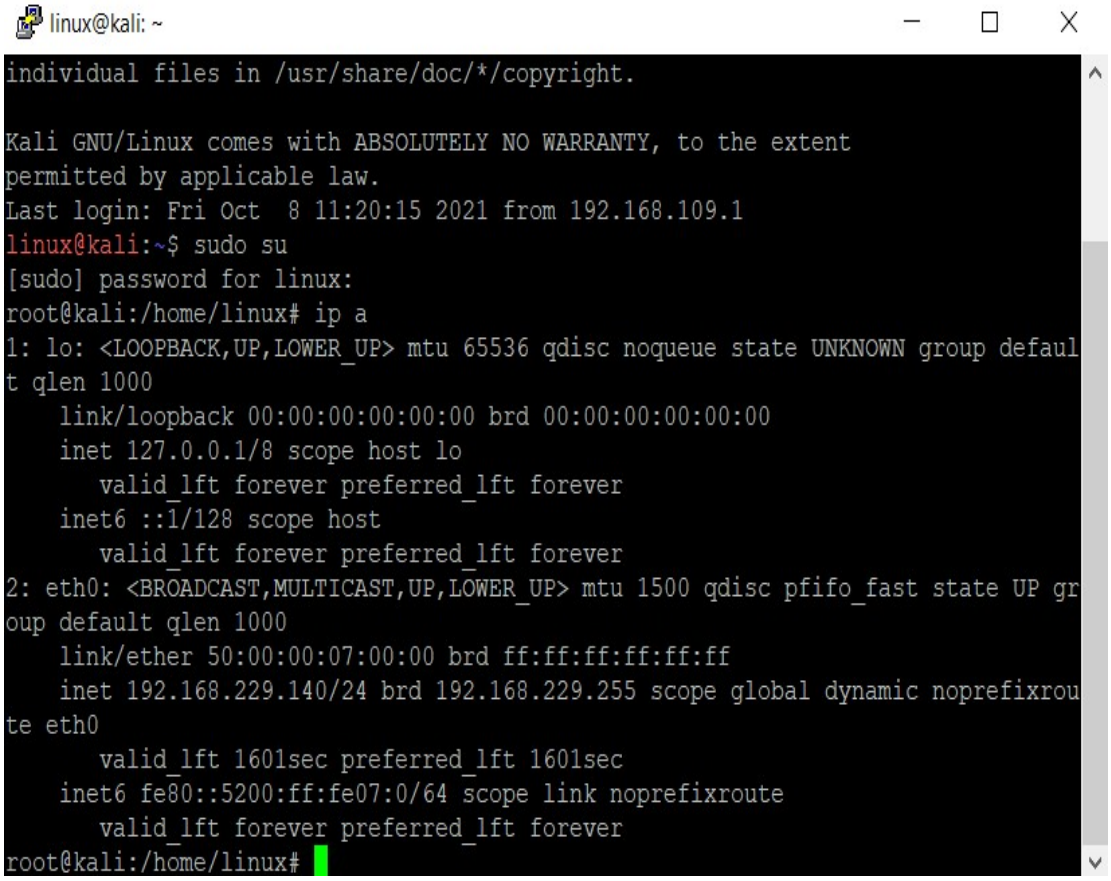
Kiểu tấn công này mục đích là do thám các thiết bị bên trong hệ thống mạng sử dụng kỹ thuật Nmap để dò được các thông tin về thiết bị, phiên bản, hệ điều hành, v.v… và sau đó tiến hành dò tài khoản mật khẩu sử dụng Hydra để bẻ khóa mật khẩu.



Hình 3.31. Sơ đồ bài lab tấn công Access-Cracking

Máy kali từ vùng ngoài outside có địa chỉ ip 192.168.229.140:

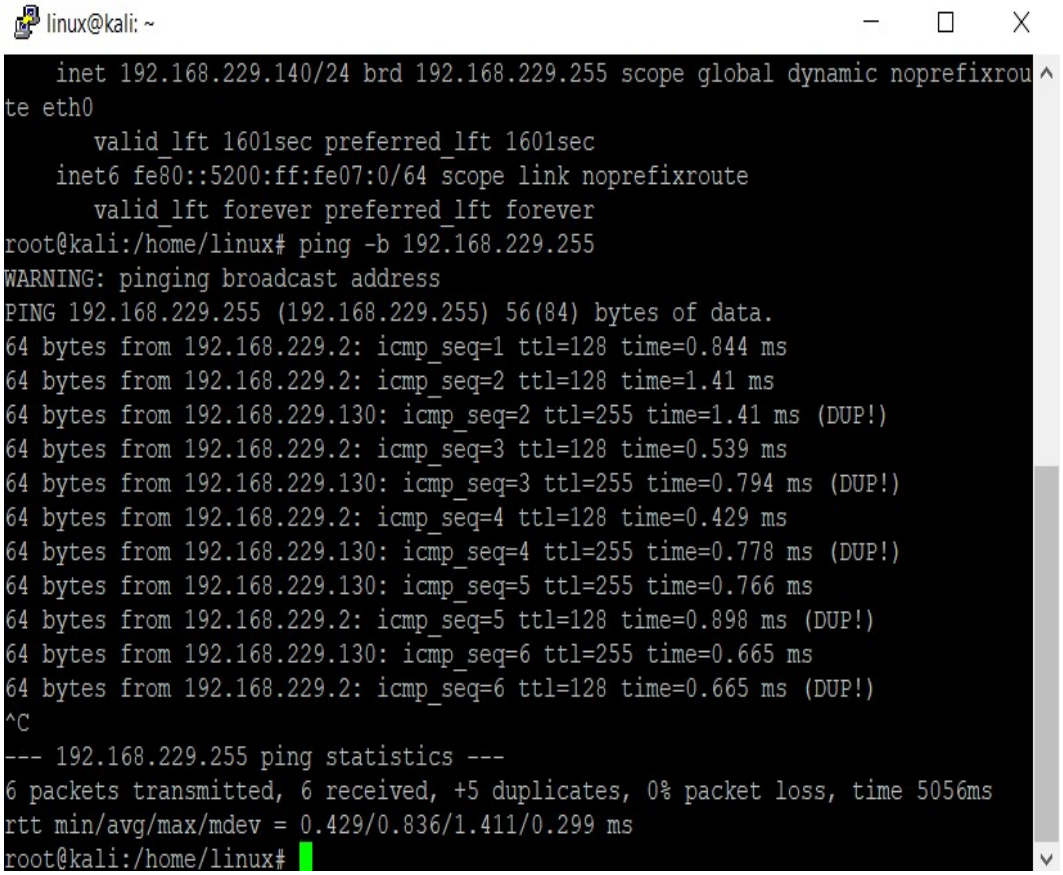
- Nhập lệnh ip a để kiểm tra thông tin IP của card mạng máy Kali linux (Attacker)



Hình 3.32. Kiểm tra địa chỉ IP của máy attacker

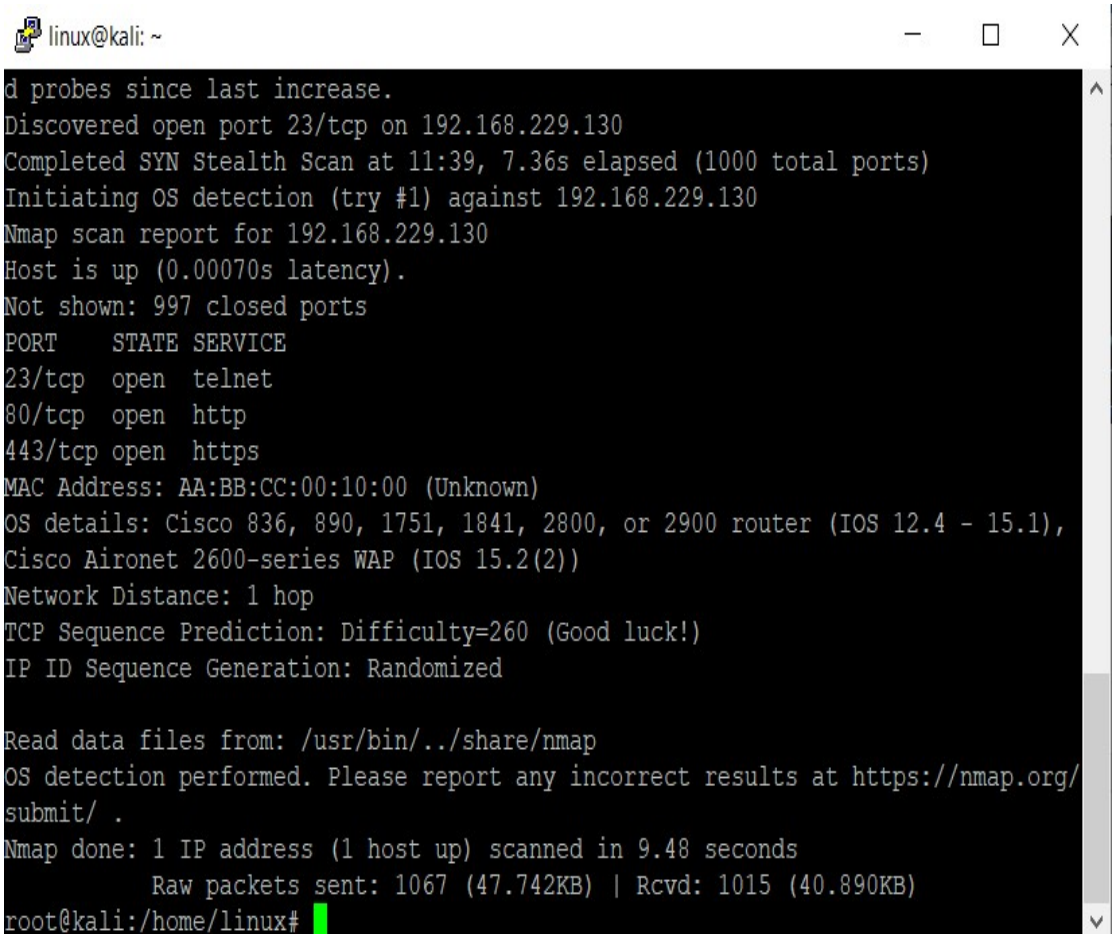
Từ máy kali thực hiện câu lệnh ping –b 192.168.229.255 (địa chỉ broadcast) để dò xem các thiết bị nào có thể trả lời, từ đó tìm ra được mục tiêu tấn công.

- Và sau đó ta thấy xuất hiện địa chỉ IP 192.168.220.130 (địa chỉ của thiết bị router GATE) trả lời:



Hình 3.33. Ping broadcast để dò ra IP của thiết bị GATE

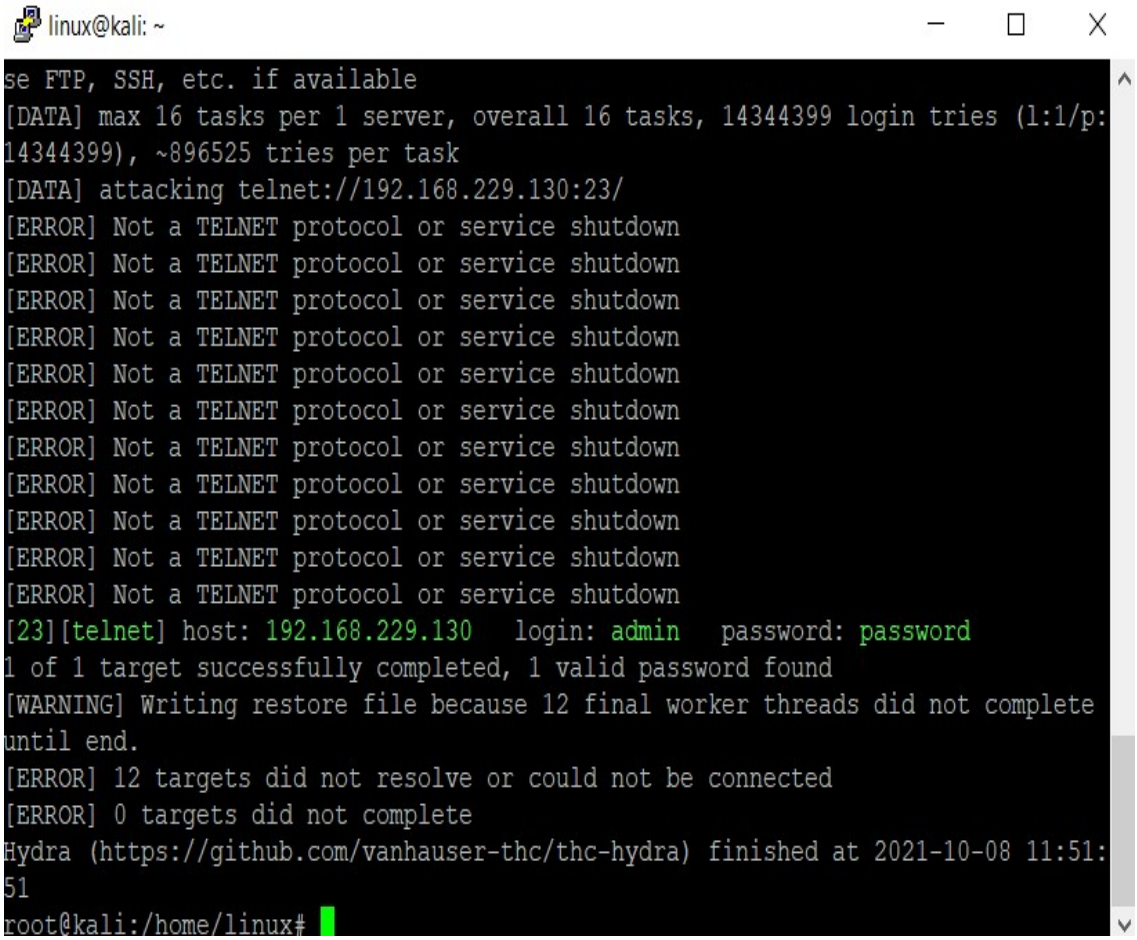
Sau đó thực hiện câu lệnh sử dụng nmap (nmap -O -v 192.168.229.130) để thực hiện xem chi tiết thiết bị của địa chỉ tìm thấy (GATE) như hệ điều hành, cổng đang mở, địa chỉ MAC…



Hình 3.34. Sử dụng Nmap dò thông tin của thiết bị thông qua IP

Phát hiện được router mở cổng 23 telnet máy kali thực hiện dò tài khoản mật khẩu để xâm nhập bằng cách nhập câu lệnh như sau:

hydra -l admin -P /usr/share/wordlists/rockyou.txt.gz telnet://192.168.229.130

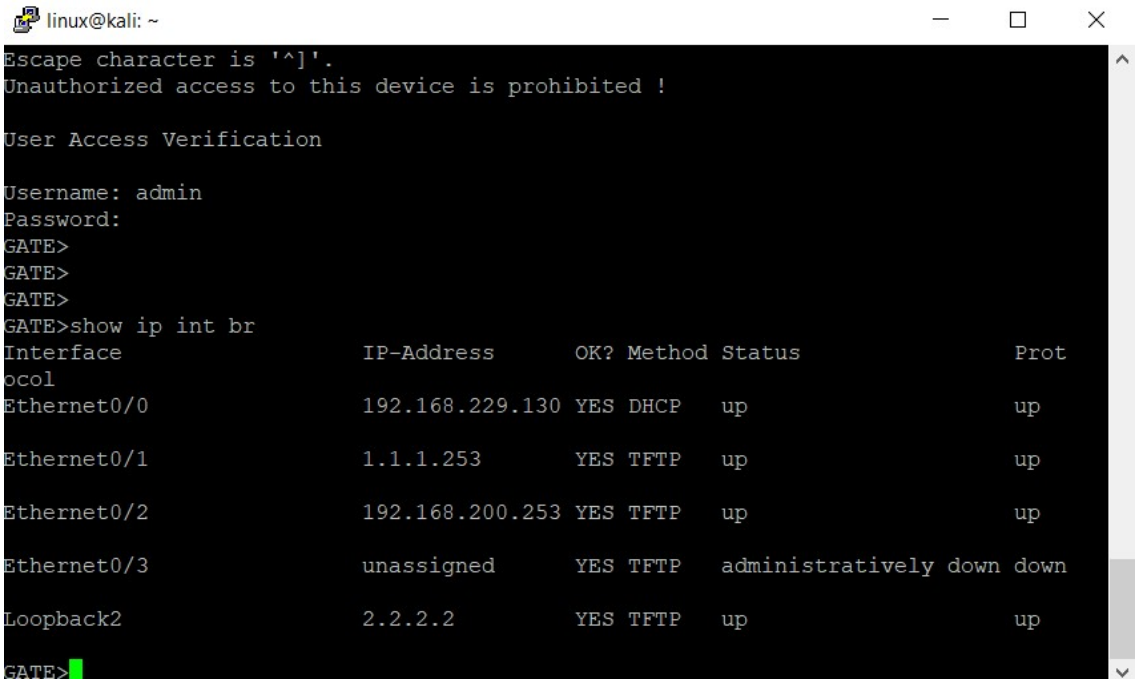


Hình 3.35. Dò thành công tài khoản và mật khẩu để truy cập vào thiết bị GATE

Sau khi dò được tài khoản và mật khẩu đăng nhập attacker thực hiện telnet vào router:

Hình 3.36. Xâm nhập vào thiết bị GATE

Telnet thành công attacker tiếp tục thực hiện câu lệnh show để xem các cổng của thiết bị có thiết bị nào kết nối đến:

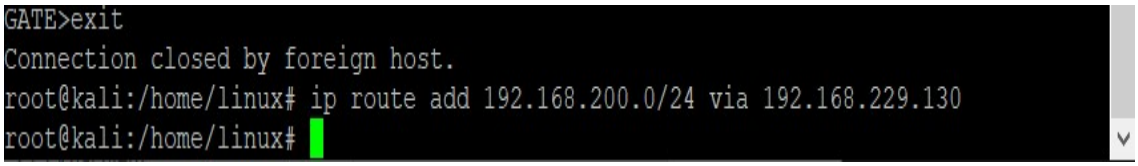


Hình 3.37. Nhập lệnh show ip để do thám được thông tin hệ thống

Sau khi hiển thị được thông tin địa chỉ ip của các cổng router attacker tiếp tục sử dụng câu lệnh:

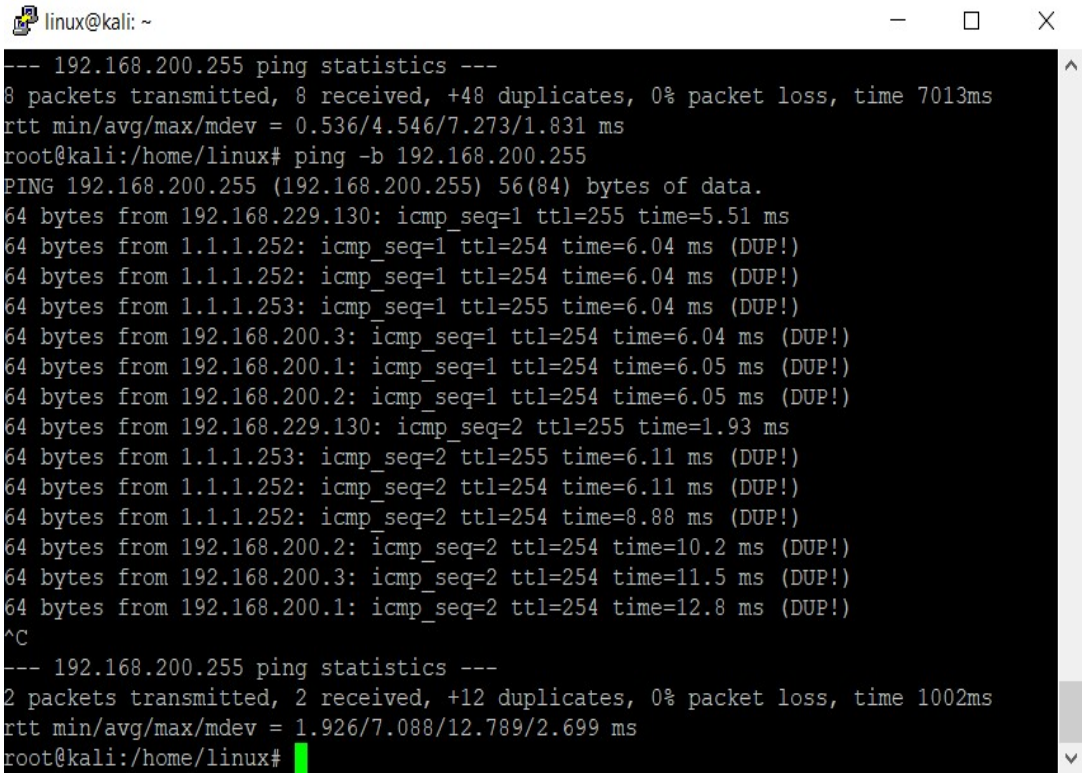
"ip route add 192.168.200.0/24 via 192.168.229.130"

- Mục tiêu để dẫn đường cho máy attacker vào trong được vùng nội bộ có dải ip là 192.168.200.0/24:



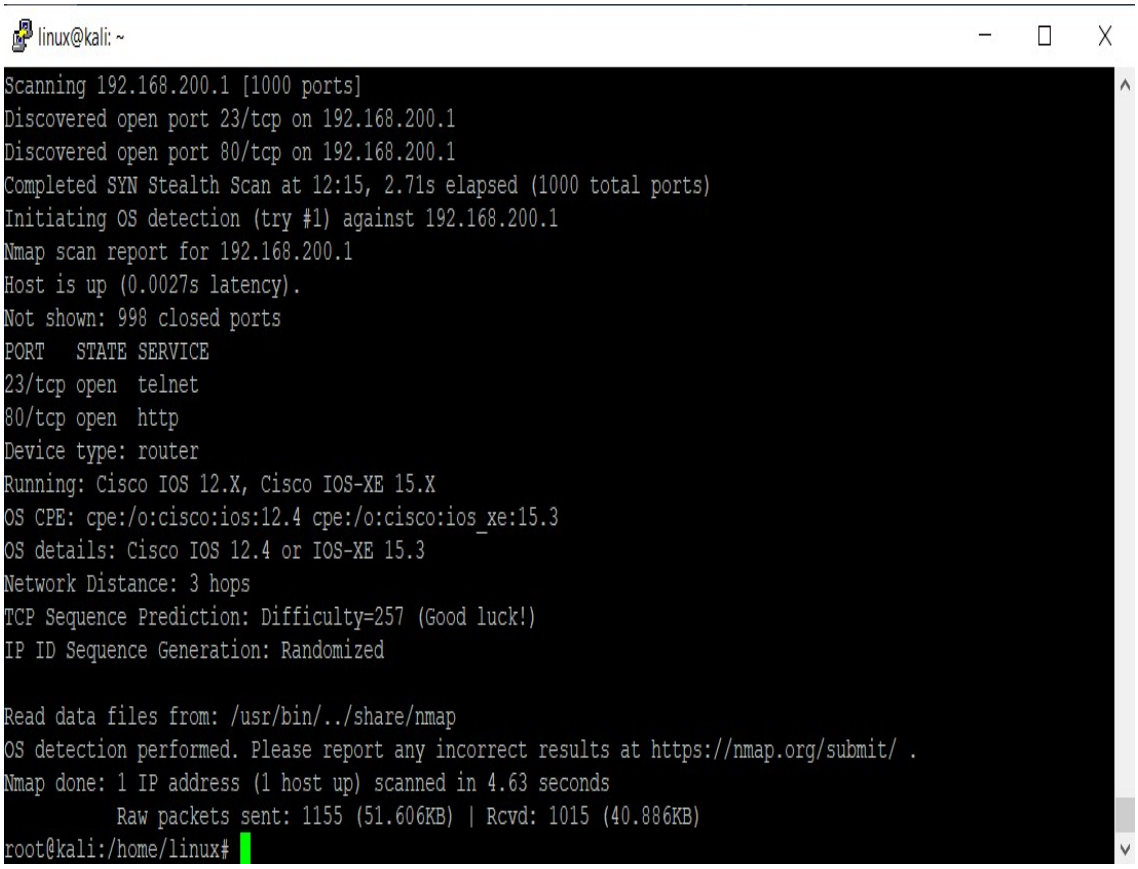
Hình 3.38. Thực hiện định tuyến cho máy attacker vào bên trong mạng nội bộ

Sau khi hoàn thành việc bypass qua vùng biên attacker tiếp tục làm lại việc ping –b đến địa chỉ broadcast 192.168.200.255 để do thám nội bộ thiết bị nào trả lời:



Hình 3.39. Tiếp tục do thám các thiết bị mạng trong nội bộ của công ty

Sau đó thực hiện do thám sử dụng nmap với 1 trong những địa chỉ ip đã trả lời để xem chi tiết thông tin thiết bị nạn nhân thông qua IP (nmap -O -v 192.168.200.1):



Hình 3.40. Tiếp tục lặp lại việc do thám các thiết bị mới trong nội bộ

Từ đây ta biết được hệ điều hành của thiết bị mới và có thể biết được thiết bị đang mở cổng bao nhiêu để thực hiện do thám và xâm nhập tiếp giống như kịch bản ở giai đoạn đầu.

3.3.3.2 Giải pháp

Giải pháp cho kiểu tấn công này là ta thực hiện lắp thiết bị tường lửa và cấu hình đúng các luật để chặn các lưu lượng trái phép truy cập vào hệ thống mạng hoặc vận hành thiết bị router tích hợp tính năng của Firewall và cấu hình các chính sách cụ thể không cho phép các thiết bị bên ngoài có thể giao tiếp được đến Router. Đặc biệt không dung tính năng DHCP để tự động cấp IP cho thiết bị mới cắm vào, chỉ sử dụng IP tĩnh và quản lý chặt chẽ danh sách IP đã cấp.

Hạn chế số lần đăng nhập và lock out nếu cố tình đăng nhập sai quá nhiều lần. Đồng thời lưu ý khi cấu hình thiết bị mới, cần xóa hoàn toàn các cấu hình mặc định, các tài khoản root, tài khoản mặc định của thiết bị, thay thế bằng các tài khoản khác có tính bảo mật cao hơn.

3.4. Hướng phát triển

Sau khi đã thực hiện thành thạo các công cụ trên hệ điều hành Kali Linux và trau dồi được kỹ năng lập trình với ngôn ngữ Python thì hoàn toàn có thể xây dựng riêng một ứng dụng hoặc một trang web để sử dụng pentest cho hệ thống. Hoặc có thể tập hợp các công cụ đánh giá an toàn thông tin cho người dùng với mục đích học tập dễ sử dụng, tham khảo và triển khai tại nơi làm việc.

3.5. Kết luận Chương 3

Trong Chương 3, luận văn đã trình bày phần thực nghiệm mô phỏng tấn công và chống tấn công với 3 phương thức.

Tấn công nội bộ theo 2 kịch bản:

- ✓ MAC-Overflow: tấn công DoS làm tràn bảng MAC
- ✓ ARP- Poisoning: tấn công Man in the Middle để chèn vào vào giữa hệ thống nhằm nghe lén thông tin

Tấn công từ bên ngoài vào hệ thống:

- ✓ Access-Cracking: Máy tấn công ở bên ngoài outside sử dụng các công cụ scan như nmap để dò ra được địa chỉ IP public của công ty từ đó do thám được thông tin của thiết bị và nghiên cứu lỗ hổng để tấn công vào vùng biên. Sau đó sử dụng công cụ Hydra để bẻ khóa mật khẩu xâm nhập vào hệ thống.

Đồng thời với mỗi phương pháp tấn công, học viên đã trình bày phương pháp để phòng chống và thực nghiệm phòng chống, kết quả đạt được là đã ngăn được phương pháp tấn công đó. Từ đó cho thấy hiệu quả của công tác phòng chống tấn công trong mạng nội bộ.

KẾT LUẬN

Trong phạm vi nghiên cứu, luận văn đã giới thiệu tổng quan về mạng nội bộ, một số công nghệ lõi sử dụng trong mạng nội bộ. Giới thiệu sơ bộ về các phương pháp tấn công vào một mạng nội bộ, đồng thời đưa ra một số giải pháp để phòng chống tấn công. Dựa trên cơ sở đó để tiến hành thực nghiệm mô phỏng hệ thống mạng nội bộ và thực hiện tấn công bằng 03 phương pháp tấn công mạng (02 phương pháp tấn công từ bên trong và 01 phương pháp tấn công từ bên ngoài).

Bám sát theo mục tiêu và nhiệm vụ của đề tài, luận văn đã thu được một số kết quả như:

- ✓ Mô phỏng được mô hình mạng thiết kế trên công cụ EVE-NG.
- ✓ Tìm hiểu được các lỗ hổng về mặt cấu hình cũng như các kiểu tấn công phổ biến.
- ✓ Thành thạo một số công cụ có sẵn trên hệ điều hành Kali Linux.
- ✓ Đưa ra được các giải pháp ngăn chặn các cuộc tấn công.

Những hạn chế còn tồn tại

- ❖ Do kinh nghiệm thực tế chưa được nhiều, kiến thức về lỗ hổng còn hạn chế, và thời gian có hạn, do vậy chưa khai thác được thêm nhiều các kiểu tấn công mới.
- ❖ Chưa vận dụng được nhiều công cụ để tạo ra mã khai thác hoặc công cụ không có sẵn để thực hiện tấn công và phòng chống.

TÀI LIỆU THAM KHẢO

Tiếng Anh

[1] D Son, Sooel; Shmatikov, Vitaly (August 14, 2017). *"The Hitchhiker's Guide to DNS Cache Poisoning"* (PDF). Cornell University. Archived (PDF) from the original on.

[2] Ramachandran, Vivek & Nandi, Sukumar (2005). *"Detecting ARP Spoofing: An Active Technique"*. In Jajodia, Suchil & Mazumdar, Chandan (eds.). Information systems security: first international conference, ICISS 2005, Kolkata, India, Birkhauser. p. 239. ISBN 978-3-540-30706-8. Computer Network.

[3] Forouzan, Behrouz (February 17, 2012). *"Data Communications and Networking. McGraw-Hill"*. p. 14. ISBN 9780073376226.

[4] Gary A. Donahue (June, 2007). *"Network Warrior".* O'Reilly.

[5] Stoneburner, G.; Hayden, C.; Feringa, A. (2004). *"Engineering Principles for Information Technology Security"*. csrc.nist.gov.doi:10.6028/NIST.SP.800-27rA

[6] Yehuda Afek, Anat Bremler-Barr, Alon Noy – (October 2, 2019), *"Eradicating Attacks on the Internal Network with Internal Network Policy"*

[7] Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). *"Towards a More Representative Definition of Cyber Security"*. Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.

Website

[1] https://www.msspalert.com/cybersecurity-guests/multi-vector-attacks-demand-multi-vector-protection/

[2] https://www.rapid.7.com/fundarmentals/vulnerabilities-exploits-threats/